

501-CD-001-004

## **EOSDIS Core System Project**

# **Performance Assurance Implementation Plan for the ECS Project**

April 1996

Hughes Information Technology Systems  
Upper Marlboro, Maryland

# **Performance Assurance Implementation Plan for the ECS Project**

**April 1996**

Prepared Under Contract NAS5-60000  
CDRL Item 076

## **SUBMITTED BY**

Mark Settle /s/	4/5/96
Marshall A. Caplan, Project Manager EOSDIS Core System Project	Date

## **APPROVED: November 25, 1994**

Comments received have been incorporated in this submittal.  
Code 505, Goddard Space Flight Center

**Hughes Information Technology Systems**  
Upper Marlboro, Maryland

This page intentionally left blank.

# Preface

---

This document, as a formal contract deliverable with an approval code 1, required Government review and approval prior to acceptance and use. It was reviewed and approved, with comments, per GSFC Code 505 contracts letter dated November 25, 1994. Comments received with the approval letter have been incorporated, and this document is now considered accepted for use; no further review is required. Future changes to this document shall be made by document change notice (DCN) or by complete revision. Any future changes must be reviewed and approved by the Government.

This document is under ECS Project Configuration Control. Any questions or proposed changes should be addressed to:

Data Management Office  
The ECS Project Office  
Hughes Information Technology Systems  
1616 McCormick Drive  
Upper Marlboro, MD 20774-5372

This page intentionally left blank.

# Change Information Page

List of Effective Pages			
Page Number		Issue	
Title		Submitted as Final	
iii through xii		Submitted as Final	
1-1 and 1-2		Submitted as Final	
2-1 through 2-4		Submitted as Final	
3-1 through 3-20		Submitted as Final	
4-1 through 4-6		Submitted as Final	
5-1 through 5-10		Submitted as Final	
6-1 through 6-4		Submitted as Final	
7-1 through 7-8		Submitted as Final	
8-1 through 8-8		Submitted as Final	
9-1 through 9-16		Submitted as Final	
AB-1 through AB-4		Submitted as Final	
Document History			
Document Number	Status/Issue	Publication Date	CCR Number
193-501-PA1-001	Pre-Approval	December 1993	
194-501-PA1-001	Pre-Approval	March 1993	94-0009
194-501-PA1-001	Original	November 1994	94-0067
501-CD-001-004	Submitted as Final	April 1996	95-0849A

This page intentionally left blank.

# Contents

---

## 1. Introduction

1.1	Identification .....	1-1
1.2	Scope .....	1-1
1.3	Purpose and Objectives .....	1-1
1.4	Document Status and Schedule .....	1-1
1.5	Document Organization .....	1-2

## 2. Related Documentation

2.1	Parent Documents .....	2-1
2.2	Applicable Documents .....	2-1

## 3. Performance Assurance Program

3.1	Management of the Assurance Program .....	3-1
3.1.1	ECS Lifecycle .....	3-1
3.1.2	Risk Management .....	3-4
3.1.3	Continuous Measurable Improvement .....	3-4
3.1.4	Metrics .....	3-5
3.1.5	Performance Assurance Scheduling.....	3-6
3.1.6	Requirements Traceability Matrix .....	3-9
3.1.7	Implementing Procedures .....	3-13
3.1.8	Performance Assurance Status Report.....	3-13
3.1.9	Surveillance of the Contractor .....	3-14
3.1.10	Audits and Reports .....	3-14
3.2	ECS Project Organization Chart and Defined Responsibilities .....	3-14
3.2.1	Quality Office Defined Responsibilities .....	3-15
3.2.1.1	Individual Roles and Responsibilities .....	3-16
3.2.2	Software Quality Assurance Facilities, Tools, and Equipment .....	3-17

3.2.3	Evaluation Techniques .....	3-18
3.2.4	Safety Assurance Planning.....	3-18
3.2.5	Nonconformance Reporting and Corrective Action .....	3-18
3.2.6	Testing.....	3-19
3.2.7	Configuration Management .....	3-19
3.2.8	Evolutionary Development .....	3-19

## 4. Performance Reviews

4.1	Review Requirements .....	4-1
4.2	Lifecycle Reviews .....	4-1
4.2.1	Preliminary Design Review .....	4-1
4.2.2	Critical Design Review .....	4-2
4.2.3	Test Readiness Review .....	4-2
4.2.4	Element Test Review .....	4-2
4.2.5	Segment Operational Readiness Review .....	4-2
4.2.6	Consent to Ship Review .....	4-3
4.2.7	Release Readiness Review .....	4-3
4.2.8	Capabilities and Requirements Review .....	4-3
4.3	Assurance Reviews .....	4-3
4.3.1	Release Initiation Review (RIR) .....	4-3
4.3.2	Preliminary Design Review/Incremental Design Review (PDR/IDR) .....	4-3
4.3.3	Critical Design Review (CDR) .....	4-3
4.3.4	Build Reviews .....	4-4
4.3.5	Test Readiness Reviews (TRRs).....	4-4
4.3.6	Acceptance Test Activity .....	4-4
4.4	Flight Mission Readiness Reviews .....	4-4
4.4.1	Ground System Operational Readiness Reviews .....	4-4
4.4.2	Flight Assurance Reviews.....	4-4

## 5. Verification

5.1	System Integration and Test (I&T) .....	5-1
5.2	Verification Infrastructure.....	5-1

5.3	Verification Procedures.....	5-4
5.3.1	Verification Methodologies .....	5-4
5.4	Hardware Verification.....	5-5
5.4.1	Custom Designed, Fabricated, or Modified Hardware .....	5-6
5.5	Software Verification .....	5-6
5.5.1	Walkthroughs or Inspections .....	5-7
5.5.2	Acceptance Test Plans .....	5-7
5.5.3	Integration Test Plan and Procedures.....	5-8
5.5.4	Software Test Reports .....	5-8
5.5.5	Critical Software Items Testing .....	5-9
5.5.6	Verification and Integration of Modified or New Software .....	5-9
5.5.7	End-to-End Test Requirements .....	5-9
5.6	Control of Unscheduled Activities During Verification .....	5-9
5.7	Verification Reports .....	5-9

## 6. Safety

6.1	Practices and Procedures.....	6-1
6.2	Applicable Codes, Regulations, and Standards .....	6-2
6.3	Implementation Plan .....	6-3
6.4	Flight Operations System Safety.....	6-3
6.5	ECS Development Facility Safety .....	6-4

## 7. Reliability, Maintainability, and Availability

7.1	General Requirements.....	7-1
7.1.1	RMA of Government-Furnished Equipment .....	7-1
7.1.2	Program Reviews .....	7-1
7.1.3	Failure Review Board .....	7-3
7.1.4	Control of Subcontractors and Suppliers .....	7-3
7.1.5	Common Use Data Base .....	7-3
7.2	Reliability Analysis.....	7-3
7.2.1	System Availability Modeling .....	7-4

7.2.2	Reliability Predictions .....	7-4
7.2.3	Reliability Allocations .....	7-4
7.2.4	Failure Modes and Effects Analysis and Critical Items List .....	7-4
7.3	Maintainability Analysis .....	7-5
7.3.1	Maintainability Predictions .....	7-5
7.3.2	Maintainability Allocations .....	7-5
7.3.3	FMEA Maintainability Information .....	7-5
7.3.4	Maintainability Design Criteria and Operating Standards .....	7-6
7.3.5	Data Collection, Analysis, and Corrective Action System .....	7-6
7.3.6	Maintainability Demonstration .....	7-6
7.4	Logistics Support Analysis .....	7-7

## 8. Software

8.1	Software Quality Assurance .....	8-1
8.1.1	Standards .....	8-1
8.1.2	Assurance Function .....	8-1
8.1.3	Documentation .....	8-2
8.1.4	Science Software Quality Assurance .....	8-2
8.1.5	Software Requirements and Design, Assurance .....	8-4
8.2	Critical Software Items Analysis .....	8-5
8.3	Software Configuration Management .....	8-5
8.4	Nonconformance Reporting and Corrective Action .....	8-6
8.5	Security .....	8-7
8.6	Software Design and Implementation Process .....	8-7

## 9. Hardware

9.1	Hardware Quality Assurance .....	9-1
9.2	Quality Assurance Plan .....	9-3
9.3	Document Change Control .....	9-3
9.4	Identification and Traceability Requirements .....	9-3
9.5	Procurement Requirements .....	9-3

9.5.1	Product Changes .....	9-4
9.5.2	Age Control and Limited-Life Products .....	9-4
9.5.3	Inspection and Test Records .....	9-4
9.5.4	Government Source Inspection .....	9-4
9.5.5	Procurements Not Requiring Government Source Inspection .....	9-4
9.5.6	Contractor QA Activity at Source .....	9-4
9.5.7	Resubmitting of Nonconforming Articles or Materials .....	9-5
9.6	Review and Approval of Procurement Documents .....	9-5
9.7	Procurement Review by the Government .....	9-5
9.8	Contractor Source Inspection .....	9-5
9.9	Contractor Receiving Inspection .....	9-5
9.10	Control of Fabrication, Integration, and Operations Phase Maintenance Activities .....	9-6
9.10.1	Fabrication and Inspection Requirements .....	9-7
9.10.2	Training and Certification for Manufacturing, Integration, Inspection, Operations, and Maintenance Personnel .....	9-7
9.10.3	Process Evaluation and Control .....	9-8
9.11	Electrostatic Discharge Control .....	9-8
9.12	Nonconformance Control .....	9-8
9.12.1	Control, Disposition, and Reporting of Discrepancies .....	9-9
9.12.2	Control, Reporting, and Disposition of Malfunctions .....	9-10
9.12.3	Reporting of Spacecraft Orbital Anomalies .....	9-11
9.13	Environmental Controls .....	9-11
9.14	Special Notices and Alert Information .....	9-11
9.15	Inspections and Tests .....	9-11
9.15.1	Planning .....	9-12
9.15.2	Inspection and In-Process Test Procedures .....	9-12
9.15.3	Inspection Activity .....	9-12
9.15.4	QA Activities During the Integration, Test, and Operations Phases .....	9-12
9.15.5	Records of Inspections and Tests .....	9-13
9.16	Maintenance Records .....	9-13
9.17	Configuration Verification .....	9-14
9.18	Metrology .....	9-14

9.19	Stamp Control System .....	9-14
9.20	Handling, Storage, Preservation, Marking, Labeling, Packaging, Packing, and Shipping .....	9-14
9.21	Government Property Control .....	9-15
9.22	Government Acceptance .....	9-15

## **List of Figures**

3-1.	Evolutionary Lifecycle Model .....	3-3
3-2.	ECS Project Organization .....	3-15
3-3.	Quality Office Organization .....	3-16
8-1.	Algorithm I&T Procedure .....	8-4

## **List of Tables**

3-1.	Team Member's Responsibilities .....	3-2
3-2.	Notional Schedule .....	3-7
3-2.	Notional Schedule .....	3-8
3-3.	PAR Traceability Requirements Matrix 1 of 5) .....	3-9
5-1.	Primary Verification Roles .....	5-3
8-1.	QA Planning .....	8-2

## **Abbreviations and Acronyms**

# 1. Introduction

---

## 1.1 Identification

This Performance Assurance Implementation Plan (PAIP), Contract Data Requirements List (CDRL) item 076, whose requirements are specified in Data Item Description (DID) 501/PA1, is a required deliverable under the Earth Observing System Data and Information System (EOSDIS) Core System (ECS), Contract (NAS5-60000).

## 1.2 Scope

The ECS PAIP outlines the steps by which the Performance Assurance Requirements will be managed and implemented, and defines the roles and responsibilities for ECS project organizations assigned to Performance Assurance. The PAIP addresses software and hardware quality assurance, reliability, maintainability, analysis, and Verification and Validation (V&V) functions. The plan describes the ECS project's approach, from performance of in-process inspection activities to participation on the Configuration Control Board (CCB), and process flow of quality requirements to the ECS Contractor Team and vendors. This document is to be used by all ECS Contract Team Members including subcontractors.

## 1.3 Purpose and Objectives

This document describes the management approach, processes, and mechanisms that the ECS Contractor employs to execute the ECS Statement of Work (SOW) and other contractual specifications. The plan serves two purposes: 1) to internally guide the operations of the Contractor's project organizations; and 2) when approved, to specify the framework for coordination between the Government, Contractor, and Subcontractors. The themes that dominate the Performance Assurance management approach are as follows:

- Concrete planning for the involvement of the various release, segments and subcontractors with measurement feedback on performance and satisfaction
- Achieving technical performance within cost and schedule constraints.

## 1.4 Document Status and Schedule

The ECS PAIP, submitted to the Government 2 weeks prior to the ECS System Design Review (SDR), is an approval code 1 document. Changes may be submitted for consideration to the Contractor and the Government under the normal change process. All changes to the document must be approved by the Government.

## 1.5 Document Organization

The document is organized into the following Nine Sections:

- Section 1, Introduction. Provides the scope, purpose and objectives of this plan.
- Section 2, Related Documentation. Sites other parent, applicable, and information documents.
- Section 3, General Requirements. Describes the basis and scope of the PAIP as well as the management approach to the assurance program and defines the responsibilities of the Quality Office.
- Section 4, Assurance Review Requirements. Defines the various Government and contractor reviews to be conducted on the program.
- Section 5, Verification Requirements. Identifies for both hardware and software, the verification and validation activities to be implemented during the development and installation of the EOSDIS data processing equipment. This section also defines the roles and responsibilities of the responsible organizations.
- Section 6, System Safety. Defines the implementation plans for both flight and ground safety programs.
- Section 7, Reliability, Maintainability, Availability. Defines the roles, responsibilities, and processes to be implemented in the areas of reliability, maintainability, availability, and logistic support analysis.
- Section 8, Software Assurance Requirements. Defines the implementation plan for software including the description of the software management and assurance approach that will be followed and the methods to be used by the Quality Office during the ECS contract.
- Section 9, Hardware Quality Assurance (QA). Covers all the quality provisions related to procurement of both hardware and software, receiving inspection and integration, identification and traceability, nonconformance control, handling, storage, and shipping. This section also deals with training, document change control, and maintenance records.

## 2. Related Documentation

---

### 2.1 Parent Documents

The following documents are the parents from which this document's scope and content are derived:

616-CD-002-001	Release B Integrated Logistics Support Plan for the ECS Project
420-05-03	Goddard Space Flight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS)
423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work
423-41-03	Goddard Space Flight Center, EOSDIS Core System (ECS) Contract Data Requirements Document
GMI 1700.2	Goddard Space Flight Center, Goddard Management Instruction: Health and Safety Program
S-302-89-01	Goddard Space Flight Center, Failure Modes and Effects Analysis for Unmanned Spacecraft and Instruments

### 2.2 Applicable Documents

The following documents are referenced within this Plan, or are directly applicable, or contain policies or other directive matters that are binding upon the content of this document.

101-CD-001-004	Project Management Plan for the EOSDIS Core System, Revision 1, DCN No. 01
102-CD-001-004	Development Configuration Management Plan for the ECS Project, Revision 1
102-CD-002-001	Maintenance and Operations Configuration Management Plan for the ECS Project
104-CD-001-004	Data Management Plan for the ECS Project, Revision 1, DCN No. 01
107-CD-002-XXX	Level 1 Master Schedule for the ECS Project (monthly)
101-110-MG2-001	Procurement Management Plan for the ECS Project
194-201-SE1-001	Systems Engineering Plan for the ECS Project

194-207-SE1-001	System Design Specification for the ECS Project
308-CD-001-005	Software Development Plan for the ECS Project
322-CD-001-001 ECS 414-CD-001-001	Interim Release 1 Integration and Test Plan and Procedures for the Project, Preliminary
322-CD-002-001 414-CD-002-001	Release A Segment & System Integration & Test Procedures for the ECS Project, Volume 1: CSMS Procedures
322-CD-005-001 414-CD-004-001	Release A Segment & System Integration & Test Procedures for the ECS Project, Volume 2: SDPS Procedures
324-CD-001-001 405-CD-001-001	Release Ir1 System and Segment Integration and Test Reports for the ECS Project available on the ECS Data Handling System (EDHS) @ <a href="http://edhs1.gsfc.nasa.gov/">http://edhs1.gsfc.nasa.gov/</a>
194-401-VE1-002	Verification Plan for the ECS Project
402-CD-001-002	System Integration and Test Plan for the ECS Project, Volume 1: Interim Release 1 (Ir-1)
402-CD-002-002	System Integration and Test Plan for the ECS Project, Volume 2: Release A
402-CD-003-001 319-CD-006-001	Release B System and Segment Integration and Test Plan for the ECS Project
409-CD-001-004	ECS Overall System Acceptance Test Plan for Release A
409-CD-002-001	ECS Overall System Acceptance Test Plan for Release B
194-502-PA1-001	Contractor's Practices & Procedures Referenced in the PAIP for the ECS Project
194-505-PA3-001	Description of Contractor and Subcontractor Audit Programs for the ECS Project
514-CD-001-004	Security-Sensitive Items List for the ECS Project
521-CD-000-XXX	Software Nonconformance Report for the ECS Project (monthly)
601-CD-001-004	Maintenance and Operations Management Plan for the ECS Project
GHB 1040.1	Goddard Space Flight Center, Goddard Handbook on Emergency Preparedness Plans and Procedures Volume 1c.
MIL-HDBK-217	Military Handbook for Reliability Prediction of Electronic Equipment
MIL-HDBK-472	Military Handbook for Maintainability Predictions
MIL-STD-470	Military Standard: Maintainability Program for Systems and Equipment

MIL-STD-471	Military Standard: Maintainability Verification/Demonstration/Evaluation
MIL-STD-882C	Military Standard: System Safety Program Requirements
MIL-STD-1388-1A	Military Standard: Logistics Support Analysis
MIL-STD-1388-2A	Military Standard: Requirements for a Logistic Support Analysis Record
MIL-STD-45662	Military Standard: Calibration System Requirements
NHB-1700.1	NASA Handbook: Safety Manual, Volume 9, Fire Protection
NASA-STD-2100-91	NASA Standard: Software Documentation Standard Software Engineering Program
SCG 72D	Hughes Space & Communications Guide: Safety, Health and Environmental Affairs Manual
None	MOSHA Rules & Regulations

In any conflict between any applicable government standard or specification listed below and this document exists, the standard or specification will take precedence.

This page is intentionally left blank.

## 3. Performance Assurance Program

---

### 3.1 Management of the Assurance Program

Project success is strongly dependent upon preventing technical and operational problems, controlling the evolutionary development. The ECS Performance Assurance program includes activities for verification, system safety, reliability-maintainability-availability, software assurance for previously developed software, custom software and COTs software and hardware quality assurance that comply with GSFC 420-05-03. A Risk management and a continuous measurable improvement (cmi) process, relating user satisfaction to the technical management process, have also been identified.

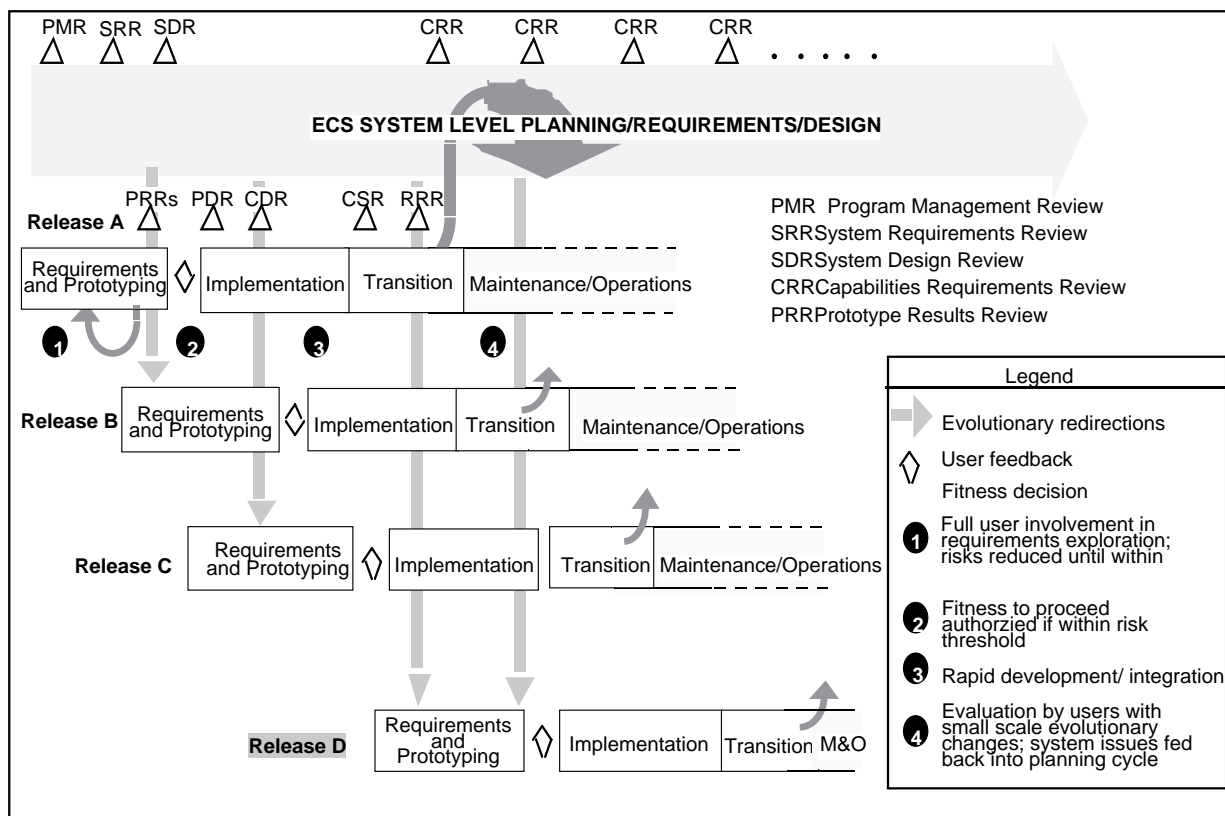
Each ECS team member has a role in Performance Assurance Implementation, which is directly related to their area of responsibilities in the Contractor Work Breakdown Structure (CWBS). Team members in the Quality Office are independent from the implementation of their respective company's tasks; rather, they perform a monitoring and audit role of those tasks in terms of adherence to standards, procedures, processes, and metrics identification. Table 3-1 reflects role allocation and provides a brief rationale for the assignment.

#### 3.1.1 ECS Lifecycle

ECS is to be accomplished in a series of incremental developments within an evolutionary lifecycle. This entails four key principles: 1) continuous system-level planning, requirements analysis, and system design activities that are responsive to user feedback from field evaluations and system performance metrics; 2) system release-specific cycles consisting of a requirements/prototyping phase followed by implementation and transition phases with the direct participation of joint teams of systems developers, Goddard Space Flight Center (GSFC), and other ECS Project representatives, including members of the ECS science user community; 3) release implementation decision points that are dependent upon the validation of predefined risk-reduction requirements; and 4) an incremental build and release process that allows changes, concurrent with implementation, after validation through rigorous technical/cost/schedule risk analyses. These characteristics are represented by the lifecycle model detailed in Figure 3-1 showing the interaction of systems planning and release development through complete release operations. Each lifecycle phase is described in the following paragraphs.

**Table 3-1. Team Member's Responsibilities**

<b>Team Member</b>	<b>Role of Quality Office in Performance Assurance Functions</b>	<b>Rationale</b>
Hughes	<ul style="list-style-type: none"><li>• Analysis of trends to identify/measure areas for process improvements (cmi)</li><li>• Identification of metrics to achieve process improvements</li><li>• Oversight and inspection at system level to ensure proper procedures are followed and in compliance</li><li>• Preparation of Performance Assurance Implementation Plans</li><li>• Management of the ECS Performance Assurance Program</li><li>• Responsibility for delivery of PA-related CDRLs</li><li>• Audit of individual subcontractor overall performance</li><li>• Attendance at assurance reviews</li><li>• System safety relating to personnel and facilities</li></ul>	Prime has overall responsibility for ECS and can evaluate and implement broad vision of program requirements
Loral	<ul style="list-style-type: none"><li>• Participation in software design reviews, software audits and inspections and attendance at software tests especially for FOS, DADS and their integration in ECS.</li><li>• Identification of process improvements for FOS, DADS</li><li>• Attendance at PA reviews and input to plans</li><li>• Providing ECS EMA support tasks</li></ul>	Design and development of FOS and DADS as well as participation in system engineering
EDS	<ul style="list-style-type: none"><li>• Inspection of RMA process for procured COTS hardware and software</li><li>• Monitoring of Audit COTS procurement standards and procedures</li><li>• Attendance at PA reviews and input to plans</li></ul>	Procurement responsibility for all COTS hardware and software
ARC	<ul style="list-style-type: none"><li>• Software assurance for ARC-developed software (toolkits)</li><li>• Attendance at PA reviews and input to plans</li></ul>	Responsibility for science algorithm development tools
ESSi	<ul style="list-style-type: none"><li>• Monitoring of procedures for user requirements collection, implementation, and training</li><li>• Attendance at PA reviews and input to plans</li></ul>	Responsibility for handling science requirements collection and tracking disposition, and training coordination and planning
NYMA	<ul style="list-style-type: none"><li>• Monitoring of compliance with standards and procedures for system interface definition and testing</li><li>• Attendance at PA reviews and input to plans</li><li>• Witness formal acceptance testing and IV &amp; V</li></ul>	Responsibility for IATO and interface with IV & V



**Figure 3-1. Evolutionary Lifecycle Model**

### 3.1.1.1 Requirements and Prototyping Phase

The goal of the requirements and prototyping phase is to specify and validate detailed requirements for the release. This goal is accomplished through a close collaboration of ECS Project Team engineers, the Science Advisory Panel, and ECS GSFC representatives. It is an iterative exploratory process that uses evaluation packages, prototypes, simulations, modeling, and other techniques to converge on the detailed requirements. Science users are enlisted to represent the needs of each discipline. This phase prepares for an explicit fitness decision (by GSFC) governed by specific thresholds of risk and science utility. Results of risk analysis are documented in a Risk Assessment Report that is updated for each Preliminary Design Review/Interface Design Review (PDR/IDR). The fitness decision occurs after PDR/IDR is successfully completed and constitutes approval to proceed into detailed design with the requirements baseline.

### 3.1.1.2 Implementation Phase

The implementation phase permits rapid development to occur based on rigorous change control mechanisms. During this phase, heavy emphasis is placed on process and product quality.

Integrated system performance is measured and optimized. Additional design, prototype migration, development, and release integration are performed.

#### **3.1.1.3 Transition Phase**

During this phase, the release is transitional from the developmental environment into operational use. GSFC determines when the release is accepted and placed into operation. This phase encompasses installation at the ECS sites, individual and distributed site acceptance testing, integration into the ECS, and independent integration verification by the Independent Verification and Validation (IV&V) contractor.

#### **3.1.1.4 Maintenance and Operations Phase**

The Maintenance and Operations (M&O) Phase provides full operational use and evaluation of the ECS release by science users, system operators, and the sustaining engineering organization. User satisfaction is continually monitored through predefined applicable metrics. A Contractor's Release Experience Report (DID 332/DV3) shall be prepared documenting the evaluations of the science advisory panels, other science and system users, and shall incorporate the ECS Project Team recommendations for subsequent follow-up and action. As the experience and understanding of operational scenarios accrues, issues that have major impact on the ECS system performance or that apply to future requirements.

### **3.1.2 Risk Management**

The ECS evolutionary development process specifically promotes user involvement and experimentation but must be controlled to operate within affordable boundaries. Rigorous risk management achieves this control. A risk management process of identification, estimation, evaluation, planning, control, and monitoring is implemented over the project organization. The deputy project manager chairs the Risk Management Panel. For a more detailed definition of the risk management processes to be implemented on the ECS Project, refer to the Project Management Plan for the EOSDIS Core System (DID 101/MG1), and the Systems Engineering Plan for the ECS Project (DID 201/SE1).

### **3.1.3 Continuous Measurable Improvement**

The Quality Office manages a cmi program ensuring that the ECS Project views experience as lessons learned and evolves toward a higher level of competency. The immediate focus areas are continued staff training and improvement of the overall technical management process, the software development process, and the process to increase software reuse.

Process improvement is a continuous cycle. The following eight-step improvement process model will be applied to the ECS project:

1. Set the expectations.
2. Assess the current practice.
3. Analyze and measure the variance between expectation and practice.

4. Propose changes that will reduce the variance and thereby improve the process.
5. Plan the integration of the improvements into the existing process and update the process definition. If a formal process definition does not exist, it should be documented now.
6. Implement the improvements.
7. Perform the process.
8. Repeat the process.

In addition to this general cmi effort, the Quality Office is supporting a Project wide effort to achieve the Software Engineering Institute (SEI) Capability Maturity Model (CMM) level 2 compliance and become ISO-9000 compliant. This effort was initiated in January of 1996 and will last approximately 11 months.

Implementation of these improvement process efforts in the various disciplines identified as sections of this plan will yield greater efficiency in producing successive system increments and will increase NASA community satisfaction.

### **3.1.4 Metrics**

The ECS Metric Goals and Activities document, dated June 1994, identifies three objectives: 1) capture and consolidate metrics that are currently being maintained, 2) document metrics that the ECS project has committed to but has not yet captured, and 3) provide a concept for the information management of metrics data. As such, this is an evolving working document. The ECS project metrics approach focuses on four key areas: early warning indicators, improved cost/schedule effectiveness, improved work processes, and progress indicators. The ECS Project Metrics Process PI (QO-1-014) specifically defines the ECS metrics program, the organizational interfaces, responsibilities, and reporting vehicles. Depending upon the type, amount, and scope of the data, metric information is maintained in a variety of systems. For small projects, such as results of inspection activities, QO personnel maintain data in Excel spreadsheets and notebooks. For larger projects, long term tracking, and all Integration and Test activities, the Nonconformance Reporting and Correction Action (NRCA) system is the primary information management system. Quality Office personnel can capture and manipulate most metrics data using the NRCA Distributed Data Tracking system (DDTs™) data base, as per PI SD-1-014.

The Quality Office is in the process of procuring the McCabe, Inc. code analysis tool known as Battlemat. This tool will be used to collect relevant metrics, including cyclomatic complexity, on the C++ code developed by ECS. These metrics will be used to assess the overall quality of the code and suggest improvements in code design and development. See Notional Schedule for delivery and implementation dates Table 3-2 of the PAIP.

Quality Office personnel from the ECS Project Team will assist the program segments/releases in identifying, analyzing, and reporting quality metrics to ensure that the program performs in accordance with contract requirements. Quality metrics will be reported at each GSFC/HAIS project review.

### **3.1.5 Performance Assurance Scheduling**

The Quality Office maintains a schedule of all audits and activities to be conducted as well as the CDRLs being prepared by or for the Quality Office. This schedule is based on the ECS Program Master Milestone schedule. A three month plan of activities is presented at the Quality Manager's Bi-Weekly meeting in the form of a notional schedule. An example notional schedule is provided in Table 3-2.

**Table 3-2. Notional Schedule**

Activity	Number of Times	Estimated Dates	Contingencies/ Dependencies
Audits			
Initial Baseline Audit	1	Completed	None
• Review Checklists			
• Audit Team Meeting			
• Conduct Audit			
• Submit Findings to QA Manager			
• Audit Team Meeting			
• Develop/Distribute Audit Report			
In-Process Audits	16	15 Working Days after completion of Audit	None
• Review Checklists		4 working days	
• Audit Team Meeting		1 working day	
• Conduct Audit		10 working days	
• Submit Findings to QA Manager		1 working day	
• Audit Team Meeting		1 working day	
• Develop/Distribute Audit Report		2 working days	
• DAAC Configuration Audit	1 per DAAC per release	1 week after software installation	Successful completion of software installation
• Software Development File Audit	1 Per Segment	After completion of INT	Completion of INT
RTM Audits			
• Periodic		As required	
• Periodic		As required	When large numbers of CCRs are input
Project Instructions (PIs)			
Nonconformance Reporting and Corrective Action (NRCA)	1	Completed	None
• Complete installation of NRCA system		Completed	
• Improve NRCA process based on current NRCA system		Completed	
• Write PI	1	Feb. 1996	Consensus on NCR severity levels
• Source Code Analysis & Metric	Continuou s	Start Feb. 96	
• Procure code analysis tool (McCabe)	1	12/30/95	NASA approval
• Install, configure, test & develop operational procedures		2/15/96	Receipt of software package

**Table 3-2. Notional Schedule**

<b>Activity</b>	<b>Number of Times</b>	<b>Estimated Dates</b>	<b>Contingencies/ Dependencies</b>
• Write PI	1	2/28/96	Installation & Configuration
DID Delivery			
• 326	Monthly	Start Jan '96	
• 506	Bi-Annual	Start March '95	
• 521 (IR-1)	Monthly	Start Nov '95	Start IR-1 Int & Test

### 3.1.6 Requirements Traceability Matrix

Table 3-3, PAR Traceability Requirements Matrix traces each PAR requirement to the applicable section in this document.

**Table 3-3. PAR Traceability Requirements Matrix 1 of 5)**

PA Requirement (GSFC 420-05-030)	PAIP Implementing Paragraph /Appendix	Implementing Organization	Auditing Organization
1.2 PA Program	3	ECS Project	Quality Office
1.3 PA Implementation Plan	1.3	Quality Office	Government, HAIS Exec Mgmt
1.3.1 Preparation of the PAIP	1.2, 1.5	Quality Office	Government, HAIS Exec Mgmt
1.3.2 Implementation Procedures	2.1, 2.2, 2.3	ECS Project	Government, HAIS Exec Mgmt
1.4 Use of previously designed and COTS HW and SW	HW - 7.1.4 9.1,9.5,9.9 SW - 5.2,5.3,5.5,9.15	FOS,CSMS, SDPS	Quality Office
1.5 Mgmt of Assurance Program	3.1	Quality Office	Government, HAIS Exec Mgmt
1.6 PA Status Report	3.1.8	Quality Office	Government, HAIS Exec Mgmt
1.7 Surveillance	3.1.9	Quality Office	Government/HAIS
1.8 Procurement	9.5	M&O	Quality Office
1.8.1 Selection of Sources	9.5.6	M&O	Quality Office
1.8.2 Requirements on Subcontractor and Suppliers	9.6	Contracts	Quality Office
1.9 Audits and Reports	3.1.10	Quality Office	Government, HAIS Exec Mgmt
1.9.1 Subcontractors and Supplier Audits	3.1.10	Quality Office	Government, HAIS Exec Mgmt.
1.9.2 Audit Reports	3.1.10	Quality Office	Government, HAIS Exec Mgmt.
1.10 Applicable Documents	2.2	Quality Office	Government, HAIS Exec Mgmt.
1.11 Abbreviations, Acronyms and Glossary	PP. AB1, AB2, AB3, AB4	Quality Office	Government, HAIS Exec Mgmt.
2.0 Assurance Review Requirements	4.1	Quality Office	Government, HAIS Exec Mgmt.
2.1 General Requirements	4.2	SMO	Quality Office

\* HW= Hardware Trace

\* SW = Software Trace

**Table 3-3. PAR Traceability Requirements Matrix (2 of 5)**

<b>PA Requirement (GSFC 420-05-030)</b>	<b>PAIP Implementing Paragraph /Appendix</b>	<b>Implementing Organization</b>	<b>Auditing Organization</b>
2.2 GSFC Review Requirements	4.2	SMO	Quality Office
2.4 System Safety	4.2	SMO	Quality Office
2.5 Contractor Assurance Review Reqmts	4.3	Quality Office	Government/HAIS
2.6 Flight Mission Readiness Reviews	4.4	M&O	Quality Office
2.6.1 Ground System Operational Readiness Review (GSORR)	4.4.1	M&O	Quality Office
2.6.2 Flight Assurance Reviews	4.4.2	M&O	Quality Office
3.0 Verification Requirements	5	SMO	Quality Office
3.1.1 System Integration and Test (I&T) Plan	5.1	SMO	Quality Office
3.1.2 Verification Procedures	5.3	SMO	Quality Office
3.1.3 Control of Unscheduled Activities during Verification	5.6	SMO	Quality Office
3.1.4 Verification Reports	5.7	SMO	Quality Office
3.2 Hardware Verification	5.4	M&O	Quality Office
3.2.1 Unit Level COTS Hardware	9.15.3	M&O	Quality Office
3.2.2 Customer Designed Fabricated or Modified Hardware	5.4.1, 9.10	M&O	Quality Office
3.2.3 Subsystem Level	9.15, 9.15.4	M&O	Quality Office
3.3 Software Verification & Validation (V&V)	5.5	Sys Eng, IATO	Quality Office
3.3.1 General	5.5.5.5.1	Releases , Sys Eng, IATO	Quality Office
3.3.2 Walkthrough or Inspections	5.5.1	Release Org.	Quality Office
3.3.3 Software Test Plans	5.5.& 5.5.2	Release Org.	Quality Office
3.3.4 Software Test Procedures	5.5.3	Release Org.	Quality Office
3.3.5 Software Test Reports	5.5.4	Release Org.	Quality Office
3.3.6 Critical Software Items Testing	5.5.5	Release Org.	Quality Office
3.3.7 Verification and Integration of Modified or New Software	5.5.6	Release Organizations	Quality Office
3.4 End-to-End Testing	5.5.7	SMO, IATO	Quality Office
3.4.1 Compatibility Test	5.5.7.1	SMO, IATO	Quality Office
3.4.2 Mission Simulations	5.5.7.2	M&O	Quality Office
4.0 System Safety	6.	FOS	Quality Office
4.1 General System Safety Requirements	6.1	SMO, M&O	Quality Office
4.2 System Safety Plan	6.2	M&O	Quality Office
4.3 Hazard Analyses	6.3	SMO	Quality Office
4.4 Hazard Control Verification	6.4	SMO	Quality Office
4.5 Reviews	6.5	SMO	Quality Office
5.0 Reliability, Maintainability, Availability (RMA) Requirements	7.	SMO	Quality Office

**Table 3-3. PAR Traceability Requirements Matrix (3 of 5)**

<b>PA Requirement (GSFC 420-05-030)</b>	<b>PAIP Implementing Paragraph /Appendix</b>	<b>Implementing Organization</b>	<b>Auditing Organization</b>
5.1 General Reqmts	7.1	SMO	Quality Office
5.2 RMA Program Plan	7.1	SMO	Quality Office
5.3 Reliability Analysis	7.2	SMO	Quality Office
5.3.1 Modeling for System Availability	7.2.1	SMO	Quality Office
5.3.2 Reliability Allocations	7.2.3	SMO	Quality Office
5.3.3 Reliability Predictions	7.2.2	SMO	Quality Office
5.3.4 Failure Modes and Effects Analysis and Critical Items List	7.2.4	SMO	Quality Office
5.4 Maintainability Analysis	7.3	SMO	Quality Office
5.4.1 Maintainability Allocations	7.3.2	SMO	Quality Office
5.4.2 Maintainability Predictions	7.3.1	SMO	Quality Office
5.4.3 FMEA Maintainability Information	7.3.3	SMO	Quality Office
5.4.4 Maintainability Design and Operating Standards	7.3.4	SMO	Quality Office
5.5 Data Collection/Analysis	7.3.5	M&O	Quality Office
5.6 Maintainability Demo	7.3.6	M&O, IATO	Quality Office
5.7 Control of Subcontractors/Suppliers	7.1.4	Subcontract Mgmt	Quality Office
5.8 RMA of GFE	7.1.1	M&O	Quality Office
6.0 Software Assurance Requirements	8.0	QA	Quality Office
6.1 General Software Assurance Requirements	8.1	Release Org., SMO	Quality Office, HITS, Government
6.1a Description of Software	8.1		Quality Office, Gvt
6.1b Management Structure/Responsibilities	8.1, 3.1,3.2, Fig. 3-2 & 3-3	EOSDIS Core System	Government
6.1c Software requirements development & control process	8.1.2,8.1.5	SMO	Quality Office
6.1d Software Design & Implementation Process	8.1.5,8.1.6	SMO Release Org.	Quality Office Government
6.1e Overview of QA process for Software Development Process	8.1.5	Quality Office	ESDIS QA
6.1f Project Software Management and Assurance re:PAR	8.1.2, 8.1.5 &SDP	Release Org.	Quality Office Govt.
6.1g Software standards & documentation	8.1.1, 8.1.3, 8.1.5	FOS, SCDO Release Org.	Quality Office
6.1.1 Documentation	8.1.1	Release Org., Sys Eng	Quality Office
6.1.2 Contractor Assurance Responsibility Software	8.1.2	Releases	Quality Office
6.2 Verification/Validation	8.2	Releases, SMO, IATO	Quality Office

**Table 3-3. PAR Traceability Requirements Matrix (4 of 5)**

<b>PA Requirement (GSFC 420-05-030)</b>	<b>PAIP Implementing Paragraph /Appendix</b>	<b>Implementing Organization</b>	<b>Auditing Organization</b>
6.3 Software Quality Assurance	8.1	Release Org.	Quality Office, HITS , Government
6.3.1 Standards	8.1.3	Release Org.	Quality Office
6.3.2 Assurance Function	8.1.2	Release Org.	Quality Office
6.4 Critical Software Items Analysis	8.2	FOS,CSMS, SDPS,SMO	Quality Office
6.5 Software Configuration Mgmt	8.3	SMO	Quality Office
6.6 Software Nonconformance Reporting & Corrective Action	8.4	SMO, Quality Office	Quality Office
6.7 Security	8.5	Quality Office	Quality Office, Government
7.0 Hardware QA Requirements	9	M&O	Quality Office, Government
7.1 General Requirements	9.1	M&O	Quality Office
7.2 QA Plan	9.2	M&O	Quality Office
7.3 Document Change Control	9.3	Bus Mgmt,	Quality Office
7.4 ID and Traceability	9.4	Subcontracts	Quality Office
7.5 Procurement Reqmts	9.5	Subcontracts	Quality Office
7.5.1 Product Changes	9.5.1	M&O	Quality Office
7.5.2 Age Control and Limited-Life Products	9.5.2	M&O	Quality Office
7.5.3 Inspection & Test Records	9.5.3	SMO, IATO, M&O	Quality Office
7.5.4 Govt. Source Insp. (GSI)	9.5.4	GSFC, M&O	Quality Office, Government
7.5.5 GSI Not required	9.5.5	M&O	Quality Office
7.5.6 Contract QA Activity At Source	9.5.6	M&O	Quality Office
7.5.7 Resub. of Non Conform. Articles or Materials	9.5.7	M&O	Quality Office
7.6 Review & Approval of Procurement Documents	9.6	M&O	Quality Office, Government
7.7 Procurement Review by the Government	9.7	GSFC	Quality Office
7.8 Contractor Source Inspection	9.8	M&O	Quality Office
7.9 Contractor Receiving Inspection	9.9	M&O	Quality Office
7.10 Control of Fab, Integ, and Operations Phase Maintenance Activities	9.10	M&O	Quality Office
7.10.1 Fabrication and Inspection Requirements	9.10.1	M&O	Quality Office
7.10.2 Training Certification	9.10.2	M&O	Quality Office
7.10.3 Process Evaluation and Control	9.10.1, 9.10.3	M&O	Quality Office
7.11 Electrostatic Discharge Control	9.11	M&O	Quality Office

**Table 3-3. PAR Traceability Requirements Matrix (5 of 5)**

<b>PA Requirement (GSFC 420-05-030)</b>	<b>PAIP Implementing Paragraph /Appendix</b>	<b>Implementing Organization</b>	<b>Auditing Organization</b>
7.12 Nonconformance Control	9.12	SMO, Quality Office	Quality Office
7.12.1 Control, Disposition and Reporting of Discrepancies	9.12.1	All Releases	Quality Office
7.12.2 Control and Disposition Reporting of Malfunctions	9.12.2	All Releases	Quality Office
7.12.3 Reporting of Spacecraft Orbital Anomalies (SOAR)	9.12.3	M&O	Quality Office
7.13 Environmental Controls	9.13	M&O	Quality Office
7.14 Special Notices & Alert Information	9.14	Quality Office	HITC, Government
7.15 Inspections & Tests	9.15	M&O	Quality Office
7.15.1 Planning	9.15.1	M&O	Quality Office
7.15.2 Inspection and In-Process Test Procedures	9.15.2	M&O	Quality Office
7.15.3 Inspection Activity	9.15.3	M&O	Quality Office
7.15.4 QA Activities During Integration, Test and Operations Phases	9.15.4	Release, SMO, IATO, M&O	Quality Office
7.15.5 Records of Inspections Tests	9.15.5	Quality Office	Quality Office
7.16 Maintenance Records	9.16	SMO, M&O	Quality Office
7.17 Configuration Verification	9.17	SMO, M&O	Quality Office
7.18 Metrology	9.18	M&O	Quality Office
7.19 Stamp Control System	9.19	Quality Office	HITC Government
7.20 Handling, Storage, Preservation, Marking, Labeling, Packaging, Packing and Shipping	9.20	M&O	Quality Office
7.21 Government Property Control	9.21	M&O	Quality Office
7.22 Government Acceptance	9.22	IATO/Quality Office	Government

### **3.1.7 Implementing Procedures**

Contractors Practices and Procedures Referenced in the PAIP (DID 502/PA1), will contain a copy of all referenced procedures in this document.

### **3.1.8 Performance Assurance Status Report**

The Quality Office is responsible for preparation of the Monthly Performance Assurance Status Report (DID 503/PA3) requirements for the contract. This report integrates the status of all performance assurance activities, whether implemented by the Quality Office or other organizational elements, on the ECS Project. Performance Assurance Monthly Status Report. In addition there are Bi-Weekly Performance Assurance Managers meeting to discuss items that are

not listed in the DID. However, assurance status information will be reported as required by Section 1.6 of the par.

### **3.1.9 Surveillance of the Contractor**

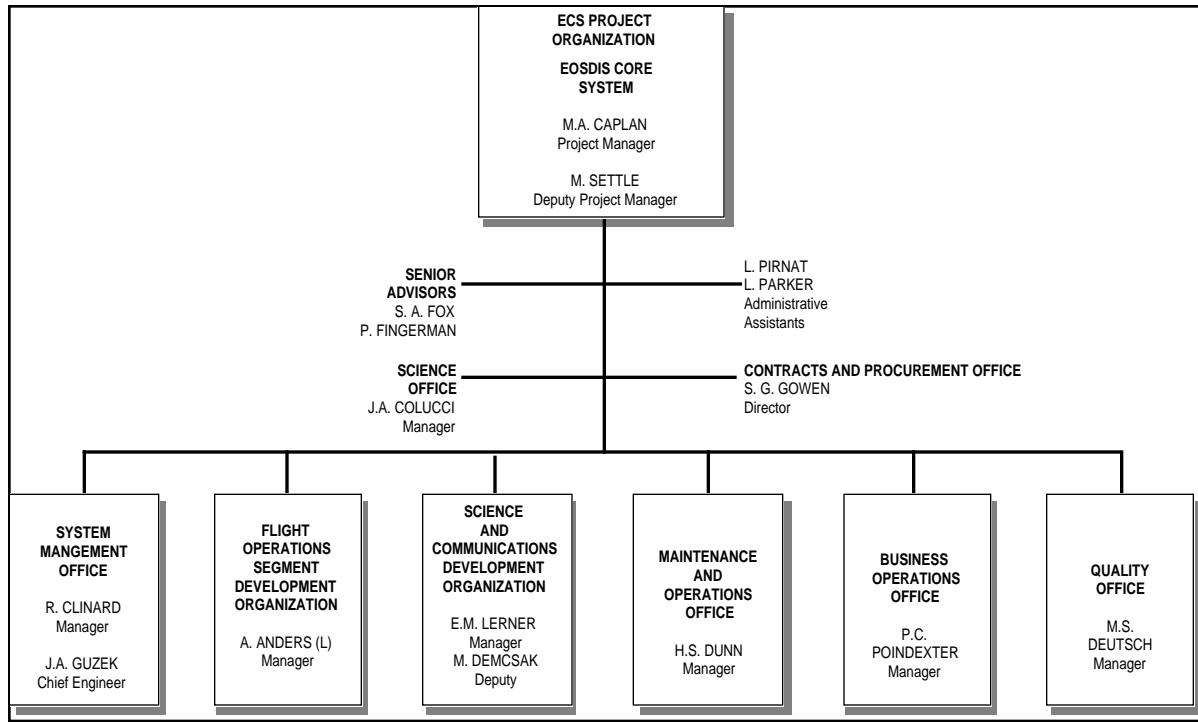
On-site work facilities are provided to Government QA representatives. Documents, records, and equipment to perform their assurance activities are provided upon request. Government representatives are encouraged to be fully participating team members with the ECS Project Team in planning and executing the PAIP. This is a key to establishing an open and cooperative relationship, providing the Government with full visibility into project status. Bi-weekly meetings are held with the contractor and the Government QA representative. Test studies, issues and concerns, and schedules are discussed at these meetings.

### **3.1.10 Audits and Reports**

A series of audits and evaluations have been selected to ensure contractor and subcontractor compliance to the performance assurance requirements on the ECS Project. The audits to be performed and the schedule of planned execution is found in the Description of Contractor and Subcontractor Audit Programs (DID 505/PA3). This document discusses Nonconformance Reporting and Corrective Action, V&V, Software Assurance; Hardware Quality; RMA availability and CM. In addition the level of planned audits may be found in the Notional Schedule provided in Table 3-1. This schedule is updated bi-weekly and forwarded to ESDIS QA during the bi-weekly meetings.

## **3.2 ECS Project Organization Chart and Defined Responsibilities**

Figure 3-2 shows the ECS project organization. Management of the performance assurance program centers on the Quality Office, which independently reports to the executive office of the Hughes Information Technology Corporation (HITC).



**Figure 3-2. ECS Project Organization**

### 3.2.1 Quality Office Defined Responsibilities

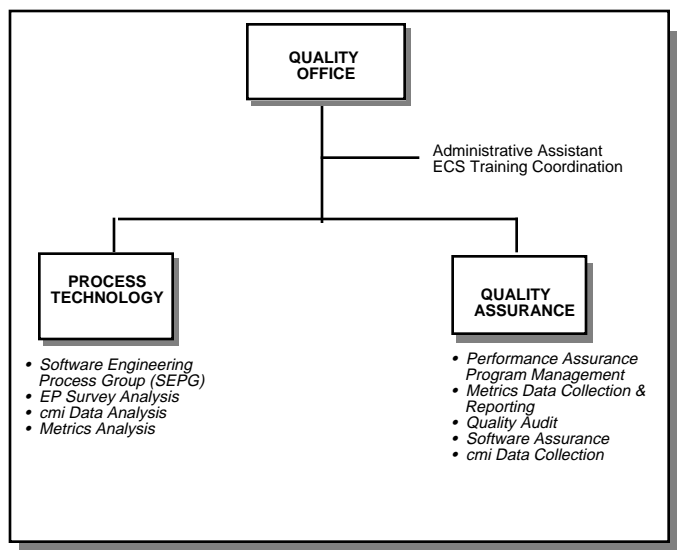
During the ECS lifecycle, the Quality Office monitors and audits processes to ensure that policies and procedures are followed and that the ECS Project Team is compliant with designated standards. The Quality Office has assigned a quality representative to each of the following ECS Project Segments: Flight Operations Segment (FOS), Interim Release 1, Release A, Release B, Tool Kit, and Evaluation Packages (EPs). The Quality representatives prepare and conduct internal segment and/or release level audits, identify process improvements, and report quality metrics. The scope of the work performed by the Quality Office is in Performance Assurance Program, WBS 7.1, and Software Quality Assurance, WBS 7.2. Further, the Quality Office coordinates the *cmi* activity for the improvement of ECS engineering and business management processes.

The Quality Office is organized into two major work activities (Figure 3-3): Quality Assurance and Process Technology. The Quality Assurance Team performs the following:

- Software QA audits and reviews.
- Hardware QA inspections, demonstrations and testing.
- Safety, flight operations, facilities, and industrial safety rules.

The Process Technology Team performs the following:

- Quality Metrics Analysis, collected from various audits conducted by each ECS Segment and analyzed for trends
- Process Improvements, made to various processes based on metric data collected and the analysis performed (the process improvement group is chaired by the Quality Office)
- Coordination of ECS Project training in the areas of *cmi*, structured software development techniques, Object Oriented Programming, and extended software engineering courses through the Motorola University.



**Figure 3-3. Quality Office Organization**

Similarly, subcontractor quality representatives report directly to executive corporate quality offices at their respective corporations. The Quality Office will be the GSFC Code 300 focal point for system quality. Figure 3-2 illustrates the Quality Office and its relationship to the ECS Program.

The Quality Office will monitor and act as an independent appraiser, as required by the EOS Program Performance Assurance Requirements (PAR). The Quality Office will assure compliance with these requirements via activities identified in the Description of Contractor/Subcontractor Audit Programs, DID 505/PA3.

### **3.2.1.1 Individual Roles and Responsibilities**

To ensure compliance in all areas of development, specific members of the QO team are assigned to the hardware and to each software segment/release. These team members have the overall responsibility for ensuring full compliance of their assigned segment/release with all applicable provisions of the PAR. Subcontractor QA personnel are full members of the QO team and

coordinate closely with Hughes personnel. They concentrate their efforts within the scope of the subcontract, but maintain responsibility for answering compliance with the PAR. QO team member responsibilities include, but are not limited to:

- Monitoring design inspections and reporting on collected inspection metrics
- Attendance at appropriate review meetings (IDR, CDR, TRR, etc.)
- Monitoring the closure of RIDs
- Monitoring source code inspections and reporting on collected inspection metrics
- Witnessing a significant sample of formal tests (Integration & Test phase)
- Reviewing documentation prior to appropriate CCB meetings
- Attendance at all appropriate CCB meetings
- Attendance at appropriate segment/release development meetings
- Continuous monitoring of status and trends and flagging potential problems
- Monitoring NRCA/DDTs™ particularly during Integration & Test and prior to CSR
- Coordinating with IV&V contractor on various witnessing and other activities (Hughes QA Only)
- Preparing monthly reports including NCR summary reports
- Various planning process, SDF, in-process and special audits as required
- DAAC configuration audits (Hughes QA only)

In addition to this primary area of responsibility, each member has secondary responsibilities such as preparing or reviewing Project Instructions, audits which span more than one area, and various special projects. As schedules and work loads dictate, team members assist each other in specific segment/release QA activities. Periodically, the QO manager reviews workloads and schedules and adjusts assignments as appropriate.

### **3.2.2 Software Quality Assurance Facilities, Tools, and Equipment**

The following facilities and equipment will be used to support the Quality Office in evaluation of the software, associated documentation, and activities:

- PC or MAC with printer, ECS office automation tools, and access to the Technical Management Data Base,
- Quality Office work area in close proximity to the ECS software development area, and
- Software coding style and naming convention verification tools.
- DDTs™ data base
- McCabe, Inc. source code analysis tool

### **3.2.3 Evaluation Techniques**

The following evaluation techniques are used by the Quality Office function to ensure that all ECS software meets performance assurance requirements.

- An evaluation is defined as the process of determining whether a product or an activity meets specified criteria.
- An evaluation technique is a type of evaluation.
- A review is defined to be an inspection or examination for the purpose of evaluating a product. The ECS Quality Office utilizes reviews to evaluate software related documentation, including management plans, requirements documents, design documents, code, and test documents.
- An audit is defined to be an examination of processes or records in order to determine their accuracy. The Quality Office utilizes audits in their evaluations of software subprocesses and Software Development Files.
- Monitoring is defined as a systematic checking of a process or activity with a view of checking only certain portions of the process or activity. The Quality Office utilizes monitoring during the evaluation of the design and code, unit test, subsystem test, and segment/release integration and test.
- Test witnessing is defined as ensuring that tests are run according to written and approved test procedures (all portions are observed). The Quality Office utilizes test witnessing during their evaluation of system acceptance tests.
- Collection and analysis of metrics, for quantitatively measuring achieved levels of quality at specific points during the program. This includes error analyses of the design and code with higher than normal error counts and trend analyses or problem reports.

### **3.2.4 Safety Assurance Planning**

During the ECS design phases, the ECS project team has performed an analyses to identify critical software items related to system safety based on the requirements and design, addressing these items in system architecture, software design, and system testing. The design addressed possible failure modes and mitigate the associated risks as determined by the analysis. Based on this analysis, the Software Critical Items List (DID 520/PA2) was prepared and approved which addressed four levels of criticality of software and the subsystems that have critical command, control, data receiving or data storing functions.

### **3.2.5 Nonconformance Reporting and Corrective Action**

A Nonconformance Reporting and Corrective Action system will be used to control nonconformance identified in software and software-related documentation. Any individual who detects a nonconformance can initiate a nonconformance report (NCR) as per PI SD-1-014. The Distributed Data Tracking system (DDTs™) is a COTs tool used to track these NCRs. The segment/release managers are responsible for assigning a technical lead to investigate the problem. If a correction to software is required, the software configuration management (SCM)

system process is used to implement and control the change. All of the organizations involved in the test program, including Quality Assurance, participate as members of the Configuration Control Board (CCB). When a change requires CCB approval the Quality Office reviews all nonconformance reports prior to CCB submission and CCB closure, to assure that all required actions have been completed. A summary nonconformance reports will be identified in the Performance Assurance Status Report (DID 503/PA3). For additional details on NRCs and DDTs™, see Section 8.4 of this documents.

### **3.2.6 Testing**

The Quality Office will monitor test environments as described in the Performance Assurance Implementation Plan (DID 501/PA1) and Description of Contractor/Subcontractors Audit Program (DID 505/PA3). During the Integration and Test phase QO personnel will witness a sample of the formal test cases from each of the threads/builds. QO will maintain a log of these witnessing activities and monitor the use of the NRCA/DDTs™ to track the NCRs submitted during the test phase. Based upon the experience gained during the IR-1 INT & Test activities, an internal QO PI is being developed to provide guidance and consistency for all future QO test witness activities.

### **3.2.7 Configuration Management**

The Quality Office performs periodic audits on both formal and incremental track developments and reports the findings to segment/release managers.

### **3.2.8 Evolutionary Development**

The Quality Office roles and responsibilities are defined in the technical note “Monitoring Concept for the Implementation of the Evolutionary Process for the ECS Project” (April 1994). The QO roles and responsibilities will be to develop checklists to monitor and track the evolvability design criteria: standard design techniques, distributed features, interpretability features and adaptive flexibility. User feedback surveys will be collected and analyzed for user satisfaction models. External interfaces described in the External Interface Control Document (DID 209/SE1 and 209/SE2) will be tracked by the QO. The QO will ensure that the requirements traceability matrix is updated to reflect unresolved or undefined external interfaces. The QO has the responsibility to identify, monitor and report risk metrics to the Risk Management Panel.

This page is intentionally left blank.

## 4. Performance Reviews

---

### 4.1 Review Requirements

The ECS Project Team is required to participate in all reviews called out in the ECS Contract Statement of Work. All reviews are linked to the ECS development lifecycle and program milestones.

For each review, the ECS Project Team:

- Submits, to the GSFC Project Office for review and approval, the required documents developed and/or updated during the subject lifecycle phase of the release being reviewed.
- Supports splinter review meetings resulting from the major review.
- Produces written responses to recommendations and action items resulting from the review, in accordance with the appropriate CDRL.
- Closes action items and discrepancies by making agreed-upon changes in the reviewed material and the products defined and controlled by them.

In addition, for reviews involving a GSFC Project Review Team, the ECS Project Team and Quality Office develop, organize, and present material to the team. Copies of visual aids and other supporting material that are pertinent to the review are submitted in accordance with the appropriate CDRL.

The ECS Project Safety Team presents, at each review, results from audits performed on the ECS System, highlighting hazards to personnel and facilities, as well as potential errors that could have adverse safety effects on the command and control of the flight system.

### 4.2 Lifecycle Reviews

The following sections describe the reviews (documented in the PAR as GSFC Reviews ) to be conducted for each ECS release. System Safety shall be an agenda item for each review.

#### 4.2.1 Preliminary Design Review

The Preliminary Design Review (PDR) for initial release and the IDRs for subsequent releases are conducted at the segment or release level of the ECS by a GSFC Project Team. Each IDR concentrates on the additional system capabilities provided by the corresponding release. Each PDR/IDR considers the following:

- The planned implementations of the corresponding portions of the overall system functions in a design of the new software and any associated additional or modified hardware.

- Proper allocation of the requirements to software components, the proposed architecture and preliminary design, and the preliminary plans for verification of the requirements by test.
- The hardware planned for purchase, custom-designed hardware, and the predicted RMA data for the ECS.

The corresponding system-level PDR/IDR, which focuses on release interfaces and segment level PDR/IDRs for each release, are Document Only Reviews. In cases where the ECS Project Team is required to present data or give a presentation, GSFC will notify the contractor 15 days in advance.

#### **4.2.2 Critical Design Review**

Critical Design Reviews (CDRs) occur at the segment level and are conducted by a GSFC Project Review Team. For each release, the CDR occurs after the software and hardware designs have been finalized, but prior to the writing of software code and the acquisition of the hardware (except for long lead-time hardware, for which early acquisition may be approved by the Government). After initial release, the CDR concentrates on the additional system capabilities provided by each new release. For software, the topics include the detailed design, its traceability to the preliminary design and to the requirements, implementation plans, data flows and interfaces, the plans for V&V, and security considerations. Hardware topics include RMA, design execution of the system functions, and the plans for testing. The corresponding system- and release-level CDR for each release focuses on interfaces and are Document Only reviews.

#### **4.2.3 Test Readiness Review**

For each release, an Acceptance Test Readiness Review (TRR) is conducted by the GSFC Project Review Team at the release and segment (FOS only) levels to review the plans for the integration and verification of the subsystems with the elements and the segments with their releases. The reviews ensure that the tests adequately verify the functional, performance, and interface requirements of the ECS.

#### **4.2.4 Element Test Review**

For each release, an Element Test Review (ETR) is conducted by the GSFC Project Review Team. This review takes place after subsystem integration and before the final Integration and Test phase. The team reviews results of segment/release tests. The review ensures that the segments tested meet segment/release requirements and operate properly and are ready for integration into the ECS system.

#### **4.2.5 Segment Operational Readiness Review**

The Segment Operational Readiness Review (SORR) concentrates on operational procedures, human interfaces, and the Operational Readiness Plan for that release. These reviews are held for each release or segment to baseline the functional capabilities, performance, and operational characteristics.

#### **4.2.6 Consent to Ship Review**

As stated in the SOW, the Consent to Ship Review (CSR) addresses the readiness of an ECS release for delivery to the operational sites for testing. Review areas include Integration and Test (I&T) results at the ECS Development Facility (EDF), the approach for installing and testing the release, and the status of test procedures for operating system integration and acceptance testing.

#### **4.2.7 Release Readiness Review**

For each release, an Release Readiness Review (RRR) is conducted by a GSFC Project Review Team at the ECS system level. The RRR addresses the readiness of the release for installation in the ECS system. Review areas include integration test results, acceptance test results, the success of new capabilities implementation, changes since the previous release, the status and adequacy of operations guides and user documentation, the status of Distributed Active Archive Center (DAAC), EOS Operations Center (EOC), and Instrument Control Centers (ICCs) interface and installation, and the plans for installation of the release into the ECS system in a manner that minimizes disruptions to ongoing service.

#### **4.2.8 Capabilities and Requirements Review**

GSFC conducts a Capabilities and Requirements Review (CRR) annually to assess the status of the ECS system capability development in meeting the existing ECS requirements and to refine design requirements for guiding further development activity.

### **4.3 Assurance Reviews**

The ECS Project Team conducts a program of planned and documented reviews within each segment at the subsystem, component, and lower level. The following sections describe the reviews (documented in the PAR as Contractor Assurance Reviews ) to be conducted for each ECS release.

#### **4.3.1 Release Initiation Review (RIR)**

This review will initiate the next release cycle. It is used to establish requirements and priorities for the next release.

#### **4.3.2 Preliminary Design Review/Incremental Design Review (PDR/IDR)**

PDR addresses the initial design of the release, and for FOS at the segment level, capabilities down to the CSU level. It marks the transition from preliminary design to detailed design. The Incremental Design Review covers how experience with the current release is being incorporated into the design for the next release. It corresponds to the PDR for subsequent releases.

#### **4.3.3 Critical Design Review (CDR)**

For each release, an intensive review of the final design and internal interfaces to evaluate the ability of the hardware and software concepts and the designs of each subsystem to successfully perform its functions under operating conditions during both testing and operation. These reviews are completed prior to the writing of software code and the acquisition of hardware

(other than long lead-time hardware for which early acquisition has been approved by the Government).

#### **4.3.4 Build Reviews**

A series of build reviews are conducted prior to implementation of each build, covering the design of additional functionality to be added to the basic design and the plans for build testing.

#### **4.3.5 Test Readiness Reviews (TRRs)**

TRRs indicate that the subsystem components are ready for release or segment I&T. This activity consist of a series of reviews. The initial review occurs when the first components of the subsystem corresponding to a release or segment thread are ready for testing.

#### **4.3.6 Acceptance Test Activity**

Throughout the acceptance test phase, results of selected increments of acceptance test activity are reviewed, focusing on the adequacy of the evaluation and the system portions evaluated to guide the need for any design modifications or test modifications. These reviews shall be conducted by personnel who are not directly responsible for the design.

### **4.4 Flight Mission Readiness Reviews**

The ECS Project Team participates in a series of GSFC readiness reviews for each EOS flight mission. The primary objectives of the flight mission readiness reviews are to ensure that all mission requirements have been met and the space and ground systems are ready to support the mission. GSFC Office of Flight Assurance (Code 300) coordinates the scheduling for these reviews. Office of Flight Assurance is responsible for notifying the participants and for the review minutes. Minutes and action items are recorded, reviewed, and signed by GSFC (Code 300 or Code 500) and the ECS contractor prior to distribution.

#### **4.4.1 Ground System Operational Readiness Reviews**

An Operational Readiness Review of the total EOS ground system is conducted by a GSFC Assurance Review Team prior to each EOS flight. The objective of this review is to certify the ECS readiness for operation.

#### **4.4.2 Flight Assurance Reviews**

Prior to each EOS mission, a series of Flight Assurance Reviews is conducted by a GSFC Flight Assurance Review Team. The following is the breakdown of the Flight Assurance Reviews:

- Mission Operations Review (MOR). To review the status of the operational interfaces with the flight system
- Flight Operations Review (FOR). To review the final orbital operations plans, as well as the compatibility of the spacecraft with the ground support equipment and ground network, including summary results of the network compatibility tests

- Flight Readiness Review (FRR). To assess the overall readiness of the total system to support the flight objectives of the mission

This page is intentionally left blank.

## 5. Verification

---

### 5.1 System Integration and Test (I&T)

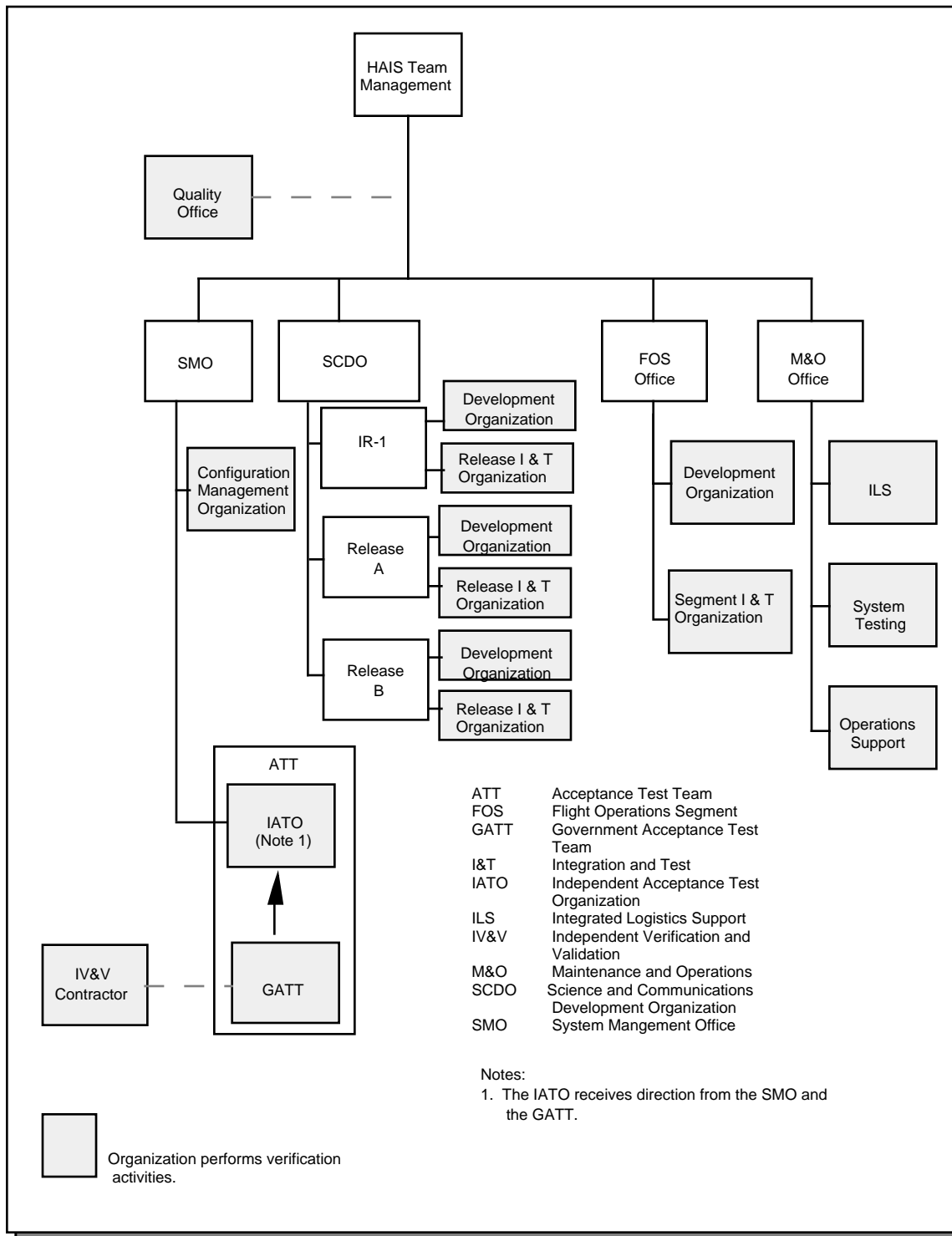
The ECS Project Team has initiated a verification program of the hardware and software for each release prior to its delivery. Figure 3-2, ECS Project Organization depicts the System I&T activities that reside with the System Management Office (SMO) office. SMO prepares, delivers, and updates an ECS System Integration and Test Plan (DID 402/VE1) for each release of the ECS (IR-1, A, B). This plan verifies specified design requirements stated in System Design Specification for the ECS System Project (DID 207/SE1). The I&T Plan is iteratively updated to reflect system evolution throughout the development lifecycle of the release, with each iteration reflecting the current stage of verification planning at the current delivery milestone.

The ECS System Integration and Test Plan includes the tests, reviews, and an analysis to verify that the item being tested meets the functional requirements in the System Design Specification for the ECS Project (DID 207/SE1). Software test plans for each ECS release are included by reference in the System Integration and Test Plan, Volume 1 and Volume 2, (DID 402/VE1). Detailed test procedures are defined in Segment & System Integration and Test Procedures, Volume 1 and 2 DID414/VE1.

The ECS Project Team prepares a test matrix for each release to summarize all tests performed within each ECS segment/release. The matrix is initially presented in the Verification Specification (DID 403/VE1).

### 5.2 Verification Infrastructure

Verification tasks are performed by the three Release development organizations, the FOS development and I&T organizations, the three Release I&T organizations, the IATO, the M&O organization, the Quality Office, the CM organization, the Government Acceptance Test Team (GATT), and the IV&V Contractor. Figure 5-1 shows the organizational relationship between these groups. The IATO and GATT jointly compose the Acceptance Test Team (ATT). There is a separate release development organization for each of the major releases and segments: Interim Release 1, Release A, Release B, Evaluation Packages, ToolKits, and the FOS.



**Figure 5-1. ECS Verification Organization**

Table 5-1 depicts the primary verification role of each organization by verification level. In addition to developing and modifying software, the release/segment development organizations perform unit testing of newly developed and heritage software. Following unit testing, the release or segment I&T organizations perform I&T activities up to and including the segment level. The release I&T organization integrates and tests all system-level functionality for an entire release. The IATO also performs acceptance testing of releases and PGS toolkits. The M&O organization supports the efforts of other organizations at the ECS sites and maintains the operational system by conducting tests during the M&O phase. The Quality Office monitors, witnesses, and audits test activities and ensures discrepancies are correctly documented and corrected. The CM organization provides baselined items for accomplishing all levels of testing and the conduct of configuration audits. The Science User Community offers operational scenarios and performance loading characteristics for acceptance testing of science data processing. The Flight Operations staff and instrument teams offer operational scenarios and performance loading characteristics for acceptance testing of flight operations systems. The GATT provides direction and oversight of IATO activities and monitors tests at other levels as desired. The IV&V Contractor performs EOS Ground System (EGS) integration testing.

**Table 5-1. Primary Verification Roles**

<b>Organization</b>	<b>Unit Testing</b>	<b>Segment/ Release I&amp;T</b>	<b>Acceptance Testing</b>	<b>IV&amp;V Testing</b>
Segment, Release Development Organizations	Perform	Support		
Segment, Release I&T Organizations	Monitor	Perform		
IATO	Monitor	Monitor	Perform	Support
M&O	Support	Support	Support	Support
Quality Office	Monitor Audit	Monitor Audit	Witness Audit	
CM Organization	Support	Support	Support	
Science User Community			Support	
GATT			Witness	Perform Witness Monitors
IV&V Contractor			Witness	Perform

## 5.3 Verification Procedures

The Verification Plan (DID 401/VE1) documents the ECS verification activities. For each test activity conducted, specific verification procedures (documented in the Verification Procedure (DID 424/VE1) are prepared to describe the configuration of the item to be tested and implementation details of the tests to be conducted.

### 5.3.1 Verification Methodologies

The verification program for the ECS employs several methodologies, including a build/thread methodology for I&T, an operational scenario methodology for acceptance testing, four methods of verifying requirements, and the analysis of test results.

- **Build/Thread Methodology**

The build/thread concept, which is based on the incremental aggregation of functions, is used to plan the segment and release I&T of the ECS. A thread is the set of components (software, hardware, and data) and operational procedures that implement a function or set of functions. Threads are tested individually to facilitate requirements verification and to isolate problems. A build is an assemblage of threads to produce a gradual buildup of system capabilities. Builds are combined with other builds and threads to produce higher-level builds. Verification of threads and builds is accomplished at progressively higher and higher levels as the release is assembled.

The build/thread approach provides two tiers of integration and testing. First-level testing, performed by the Segment/Release I&T organizations, verifies consistency to the designs and assigned functionality of subsystems and segments. Second-level testing, is also performed by the Release I&T organization, combines segment-level builds/threads into a system release and verifies ECS design against overall requirements and user needs. Both levels of testing can be performed in parallel.

- **Operational Scenario Methodology**

Acceptance testing utilizes the expertise of the science user community in developing operational scenarios to verify the ECS Level 3 requirements. In preparing for acceptance testing, the IATO solicits ideas from the science community on developing these scenarios. The science user community offers test scenario candidates that are reviewed by the IATO and GATT. These three organizations work together to refine the operational scenarios and incorporate them into acceptance testing plans and procedures.

- **Verification of Requirements**

Four standard verification methods are used to verify the ECS: inspection, analysis, demonstration, and test.

- **Inspection.** The visual, manual examination of the test item and comparison to the applicable requirement or other compliance documentation, such as engineering drawings.

- Analysis. Technical or mathematical evaluation based on calculation, interpolation, or other analytical methods. Analysis involves the processing of accumulated data obtained from other verification methods.
- Demonstration. Observation of the operation of the verification item in a controlled environment to yield qualitative results.
- Test. The execution of the verification item according to specific, predefined procedures to yield quantitative results.

The distinction between the demonstration method and the test method is subtle. The emphasis regarding the *demonstration* method is on *observing* the operation of a test item that is primarily *qualitative*. The emphasis regarding the *test* method is on *executing* a test item that yields *quantitative* results. The demonstration method usually does not require the use of elaborate instrumentation or special test equipment and does not necessarily generate output data or quantitative results. For COTS hardware and associated COTS software, e.g. operating systems, demonstration is the most common verification method. The test method always generates quantitative results including null results. The success/failure of a test item associated with the demonstration method can be determined by simple observation of the qualitative results. For the test method, the pass/fail criteria requires, as a minimum, a quantitative comparison.

For a given requirement and verification level, multiple verification methods might be employed. The method(s) chosen is(are) determined by the nature of the requirement and cost/time involved and discussed further in the Verification Plan (DID 401/VE1).

- Analysis of Test Results

Post-test analysis includes data reduction and comparison of actual results against expected results. These analyses are accomplished primarily by those organizations responsible for executing the respective tests, e.g., the Segment/Release I&T organizations perform post-test analyses for segment tests and the IATO for acceptance testing. All data reduction output is reviewed for completeness and consistency and marked for positive identification. Materials used to identify results and investigate possible anomalies include test output, logs and other records of events, discrepancy reports, data reduction material, and records of other test sessions. The Verification Plan (DID 401/VE1) presents detailed descriptions of post-test analyses responsibilities for each organization.

## 5.4 Hardware Verification

Each unit of the ECS COTS hardware is verified against the procurement specification requirements. Activities include verification of performance parameters through inspection, analysis, demonstration, and/or test. Reliability and maintainability data will be verified by review and analysis. The ECS Project Team obtains the manufacturer's diagnostic software, when possible, to verify operating system software and peripheral hardware. Automated Data Processing (ADP) hardware covered by applicable Government Site Acceptance (GSA) criteria is acceptance tested in accordance with those criteria. Section 9 discusses hardware verification,

plans, and procedures. The Description of Contractor and Subcontractor Audit Plans (DID 505/PA3) provides the planned audits by which the Quality Office verifies compliance with the performance requirements.

The hardware verification performed throughout the ECS project includes the following:

- Vendor in-process inspection and test
- Receiving inspection and demonstration
- Surveillance inspection
- QA activity during I&T
- Analysis of maintenance and nonconformance reporting

The hardware verification methods are further discussed in Section 9.

#### **5.4.1 Custom Designed, Fabricated, or Modified Hardware**

The ECS Project Team does not anticipate the use of custom designed, fabricated, or modified hardware. However, if custom designed, fabricated, or modified hardware is required, applicable hardware tests at the unit, component, and/or system level will be conducted to determine that the hardware meets specified requirements and is free of workmanship defects as described in NASA Handbook (NHB) Workmanship Standards. Upon identification of requirements for custom designed, fabricated, or modified hardware, the Quality Office coordinates a verification plan with GSFC Performance Assurance personnel.

### **5.5 Software Verification**

Software segment and release test plans and procedures are reviewed by the IATO and Product Assurance for completeness and discrepancy resolution. The Quality Assurance Team witnesses test executions and participates in reviews and analyses. The software tests are included by reference in the Integration & Test Plan (DID 319/DV1).

Upon verification, the software is integrated at the release or segment level. The integration plans and procedures are documented in the Segment Integration & Test Plan (DID 319/DV1) and Segment Integration & Test Procedures (DID 322/DV3). Detailed test procedures are defined in DID414/VE1, ECS System Integration and Test Procedures. QA monitors and witnesses tests and ensures discrepancies are recorded in the NRCA discrepancy tracking data base. IATO witnesses and evaluates the integration tests and participates in test reviews and analysis. Test results are documented in accordance with the applicable CDRL Items. Software assurance activities are discussed in Section 8.

For each release, SMO prepares a test matrix summarizing all tests performed within each ECS segment or release. The Quality Office ensures discrepancies are documented and potential risks are identified to the ECS Contractor Management Risk Committee.

The verification processes used to ensure that software is correct and meets its requirements include the following:

- Software code walkthroughs or inspections
- Software test plan
- Software test procedures
- Software test reports

### **5.5.1 Walkthroughs or Inspections**

Software walkthroughs and/or formal inspections shall be conducted during the design and code development phase in accordance with Project Instruction (SD-1-004,) Software Inspections. A member of the QO team attends all design and code inspections. The Quality Office maintains records of all formal inspections and collects metrics on the results of these inspections as per the Software Inspections PI (SD-1-004). The metrics are periodically reported to the QO manager and are forwarded to ESDIS QA at bi-weekly meetings. The results of these findings may also be reported at the Monthly Progress Review. The Quality Office audits each release/segment to ensure walkthrough and/or inspection records are maintained. The Quality Office, as a member of the ECS CCB, has review and approval authority over all software products.

### **5.5.2 Acceptance Test Plans**

Software Acceptance test plans are developed at the segment level and verified by IATO and the Quality Office. The Quality Office verifies Acceptance Test process as per DID415. Each release organization is responsible for software testing and notifies the Quality Office, and prior to test execution. Integration test plans, procedures, and reports are developed at the release level.

The Quality Office, and IV&V contractor in their role as part of the IATI, monitor test implementation, reviews, and analysis. The ECS Project maintains a Nonconformance Reporting and Corrective Action (NRCA) system for tracking software problems, using the DTTs tool as per 3D-1-104.

The software acceptance tests are documented as part of the ECS Overall System Acceptance Test Plan (DID 409/VE1) and include the following:

- Description of the software to be tested
- Purpose of each software acceptance test
- Sequence of each series of tests
- Schedule of tests to be performed
- Definition of all tests scheduled
- Definition of test support requirements
- Facility requirements

- Criteria for acceptance/rejection
- PTE and Calibration Date
- Other pertinent data

Software test plans at all levels are updated as software requirements are updated. Any changes or updates to the software tests plans are included as part of each applicable review listed in Section 4, as well as descriptions of regression tests planned to verify that the change did not affect the stability of existing software items.

### **5.5.3 Integration Test Plan and Procedures**

Requirements and design features are demonstrated during the integration and test phase. The test procedures detail the steps, procedures, and special instructions necessary to conduct tests. The specific plan and procedures for integration and test of each ECS release is documented in the Integration and Test Plan and Procedures for the ECS project. (DID322/414). These documents shall also contain a verification traceability matrix which maps level 4 requirements to specific test cases. At the conclusion of the integration and test phase, a test report shall be issued. The Integration and Test Plan and Report for the ECS project (DID324/405) shall contain all test results, updated test procedures and test results analysis. Each of these reports shall also contain any updates or corrections to mapping of level 4 requirements to test cases. To that end, the Quality Office monitors the DDTs™ system and procedures a report of all nonconformances discovered during the integration phase (DID521). QA roles and responsibilities are to verify that all test procedures are accurate and correct, witness and monitor test activities, and ensure that discrepancies and anomalies are reported.

### **5.5.4 Software Test Reports**

The software test reports include, at a minimum, the following items:

- Identification of the software item tested
- Type of test (release/segment/subsystem, integration, etc.)
- Design requirements
- Actual test results compared to expected results
- Summary of discrepancies found
  - number
  - type
  - criticality/priority
- Test scenarios for unsatisfactory performance
- Interface tests

System I&T reports are prepared in accordance with Verification Specification (DID 405/VE3), and acceptance test reports are reported in accordance with ECS Overall System Acceptance Test Report (DID 412/VE2).

### **5.5.5 Critical Software Items Testing**

During the ECS design phases, the ECS Project Team performs analyses to identify critical software items based on the requirements and design. The design addresses possible failure modes and mitigates the associated risks as determined by the analysis. All critical software items identified during analysis are included in the Software Critical Items List (DID 520/PA2). Software tests are developed by the segments/release, System I&T, and acceptance functional groups. These tests assess the potential effects of the risks identified and the measures used to minimize them. Where applicable, safety issues identified in the hazard analyses are included in the software tests.

### **5.5.6 Verification and Integration of Modified or New Software**

During the operational phase, integration tests are performed to ensure the modified or new software does not impact ongoing ECS operations during testing.

### **5.5.7 End-to-End Test Requirements**

The ECS Project Team supports end-to-end requirements as described in the following sections.

#### **5.5.7.1 Compatibility Tests**

The ECS Project Team supports compatibility tests conducted by the EOS Spacecraft Contractors.

#### **5.5.7.2 Mission Simulation**

The ECS Contractor supports mission simulation tests conducted by the EOS Spacecraft Contractors.

## **5.6 Control of Unscheduled Activities During Verification**

The ECS Project Team documents the Procedure for Control of Unscheduled Activities during Verification (DID 404/VE1). These procedures identify individuals authorized to make real-time decisions during test activities that may require temporary fixes to conclude the test. The procedures will also define the necessary steps to document and test the fix.

## **5.7 Verification Reports**

Verification reports are provided for testing activities in accordance with the applicable DID. Hardware test reports include, at a minimum, the following information:

System verification reports summarize the system I&T, acceptance tests, or any retest activities. At a minimum, the reports include the following items:

- Identification of the system item tested
- Type of test
- Design requirements
- Conformance of the test results to the expected results
- Number, type, and criticality of discrepancies
- Test scenarios
- Verification activities of functionally related system items

The detailed test results are documented by release, segment, and integration and are verified by the IATO through acceptance tests.

## 6. Safety

---

### 6.1 Practices and Procedures

Unplanned events which result in injuries, industrial illnesses, and property damages cause negative impact to programs, interruptions to the orderly process of performance, and affect efficiency, reputation, and cost management for the ECS Project Team and our customers. The increased cost of risks, losses, and liabilities is also a detriment to sound management practices.

Accident producing events can and must be controlled with organized, uniform safety and health programs for all of ECS Program development and operations. Effective leadership at all levels of management from the top executives to our lowest level staff member is mandatory. Positive response from all government and contractor staff is essential for a productive safety and environmental health program.

A safety and environmental health program has been established to provide a safe and healthful work environment for our employees and community environs. We will extend our practices as required to encompass the entire scope of the ECS program contract within the bounds of NASA standard practices. To implement the program, a Hughes Aircraft Company manual of Safety and Environmental Health, which is an extension of the Company's Policies and Procedures Manual, has been developed and will be adapted for ECS purposes. The manual provides guidelines and procedures for implementing safety practices for all of the ECS contract staff.

These standards and practices will be augmented with the results of analysis performed during ECS development and operational evolutions concerning Failure Modes Effects Analysis (FMEA), Maintainability, Availability, Training, Certifications, and necessary contingencies and plans. This plan shall be maintained with the latest updates to information on the following as applicable:

- a. system safety organization, interfaces, and responsibilities
- b. milestone schedule of all major system safety activities which shows their time phasing with other related major activities
- c. system safety methodologies
- d. internal and external safety review process
- e. safety review of test and operating procedures
- f. hazardous operations surveillance
- g. accident investigation and reporting
- h. training and certification
- i. safety audits
- j. monitoring of subcontractors
- k. documentation to be provided (i.e., CDRL)

- l. procedure for reporting problems and activity status; and
- m. industrial safety engineering responsibilities, functions, and their interfaces with the safety program

## **6.2 Applicable Codes, Regulations, and Standards**

Hughes Safety and Environmental Health policy states that maintaining a safe, healthy working environment is a prerequisite to running a successful program that satisfies ECS mission requirements. Part of the effort involved in achieving that objective is compliance with legally required safety and health codes and regulations. Against this background of legal requirements is the set of ECS requirements which are still evolving, the industrial practices, NASA standards and instructions, and regional codes governing the use of commercial facilities. The order of precedence will be first to the applicable laws and regulations, then the ECS contract requirements, followed by Hughes standard practices, and lastly good engineering judgment based on analysis of the situation in consultation with the customer organization. Safety, Health, and Environmental Affairs.

Subordinate to any contractually required organization and interface requirements, the Hughes Space Communications Group (SCG) Practice No. 3-0-11 sets forth a generalized format for responsibilities of supervision and organizations for safety and health related to personnel, property, and protection of the environment. Supervisors at all levels ensure that operations within their assigned area of responsibility are safe and healthful. Supervision assures that adequate safeguards are provided, employees are trained regarding the hazards of their tasks and the environment; periodic safety inspections are conducted with necessary corrective measures taken, and the safety requirements are enforced.

The ECS Safety, Health, and Environmental Affairs (SHEA) organization is established under the Maintenance and Operations office to support all ECS facilities and operations as well as off site operations. Contractor and subcontractors are required to comply with government safety requirements as well as the ECS facility safety practices and procedures when at these facilities. The organizational activities of SHEA include the following:

- a. Safety Engineering, Industrial Hygiene, Health Physics, Fire Prevention/Protection, Hazardous Waste Management, and Environmental Compliance
- b. Providing information, interpretation of standards, consultation, and training
- c. Audit facilities and operations; review and approve facility and operations plans and procedures; and review accident reports and investigate as necessary
- d. SHEA personnel are authorized to cause immediate cessation of any operation involving imminent hazard to personnel, property, and/or the environment.

An ECS program-level SHEA committee is established to provide an upper level focal point for legal, regulatory, and operational safety, health, and environmental issues that affect ECS. SHEA instructions and bulletins are authorized and are approved by the QA Manager. Periodic audits of the ECS SHEA Program are made internally, by customer IV&V, and by corporate SHEA representatives.

## **6.3 Implementation Plan**

The System Safety Implementation Plan (SSIP) shall comply with all the specifications of the EOS Performance Assurance Requirements for ECS (GSFC 420-05-03). This plan will include the organization, responsibilities, resources, interfaces, specific activities, schedule milestones, and products for the System Safety Organization. The statement of how the safety requirements will be met will be incorporated into the ECS Product Specification.

Early and continued analysis of potential mishaps with the most severe consequences, is our major approach to protecting flight hardware, avoiding irretrievable major loss of science data, and protecting personnel from hazards. We will assemble a list of these potential mishaps, review their resolution/mitigation status, and add items as they may emerge. These consequential mishaps then become the subjects of the FMEA.

## **6.4 Flight Operations System Safety**

There are several factors involved with Flight Operations Safety. The Flight Operations System, the Flight Operations Team (FOT), external Flight Operations interfaces, and the actual EOS spacecraft are all factors in Flight Operations Safety. The Quality Office will ensure that elements of these factors are identified and tested as critical items in conjunction with the PAR.

The FOS Command Management Subsystem (CMS) Constraint Database provides the initial safety measurement for real-time operations. All commands sent to a EOS spacecraft are subject to the constraints and conditions identified in this database. This ensures the integrity of all commands sent to a spacecraft. Prerequisite states and conditions are verified prior to commanding to prevent erroneous command from being sent to a spacecraft. Real-time critical commands are also validated by the CMS Constraint Database and require additional levels of authorization to transmit these commands.

The FOT provides the human interface between the ground system and a spacecraft. Specific procedures and constraints are in place and will be used by the FOT to prevent erroneous commands from being sent to a spacecraft and to ensure that solid engineering techniques are used to maintain spacecraft health and safety. The FOT will also conduct extensive trending analysis of spacecraft telemetry. This trending analysis will aid in predicting potential spacecraft problems prior to their occurrence.

There are several external Flight Operations interfaces which can affect Flight Operations Safety. These include experimenter command loads, communications links, and Flight Dynamics Facility provided data. Each external interface will be tested prior to launch and prior to the implementation of any interface changes that will affect Flight Operations. External Interfaces will be regulated through "Interface Control Documents."

Each EOS spacecraft will contain on-board software which will notify the Flight Operations System and FOT of anomalous conditions aboard the spacecraft. The FOT will respond to any spacecraft anomalies, with concurrence from the Mission Operations Manager (MOM) with predefined procedures to correct the anomalies and ensure spacecraft safety.

## **6.5 ECS Development Facility Safety**

Hughes operating procedures (Company Practice 5-0-7: System Safety) require a safety plan for each facility. This plan includes topics such as fire and earthquake procedures, emergency medical services, warnings/alarms, emergency switches, lights, and evacuation routes.

We have prepared two plans that fulfill the ECS Development Facility (FDF) safety assurance requirements in the ECS Development Facility Automated Information System Disaster Recovery Plan and the Emergency Preparedness Plan which were written in response to the Unclassified Automated Information Security Plan for the ECS Project.

System safety will be on the agenda for all risk panel and design reviews.

## 7. Reliability, Maintainability, and Availability

---

### 7.1 General Requirements

The RMA tasks identified by Work Breakdown Structure (WBS) elements 7.3 and 7.4, this section, and the PAR, GSFC 420-05-03, are performed by the System Management Office starting early in the ECS design and continue throughout the ECS lifecycle. This approach ensures that the ECS design is reliable, supportable, and has the lowest LCC. The objectives of this section are to ensure that all RMA requirements are satisfied (special attention is given to the Operational Availability ( $A_O$ ) strings), RMA trade studies are performed, ECS is operational and supportable, and the LCC is minimized. This ECS program design is based on COTS hardware; therefore, the RMA analysis is performed using data provided by the COTS vendors. As the program matures, the analysis is updated using observed data.

Figure 7-1, ECS RMA Schedule, shows the corresponding schedule related to the RMA tasks and the ECS program milestones.

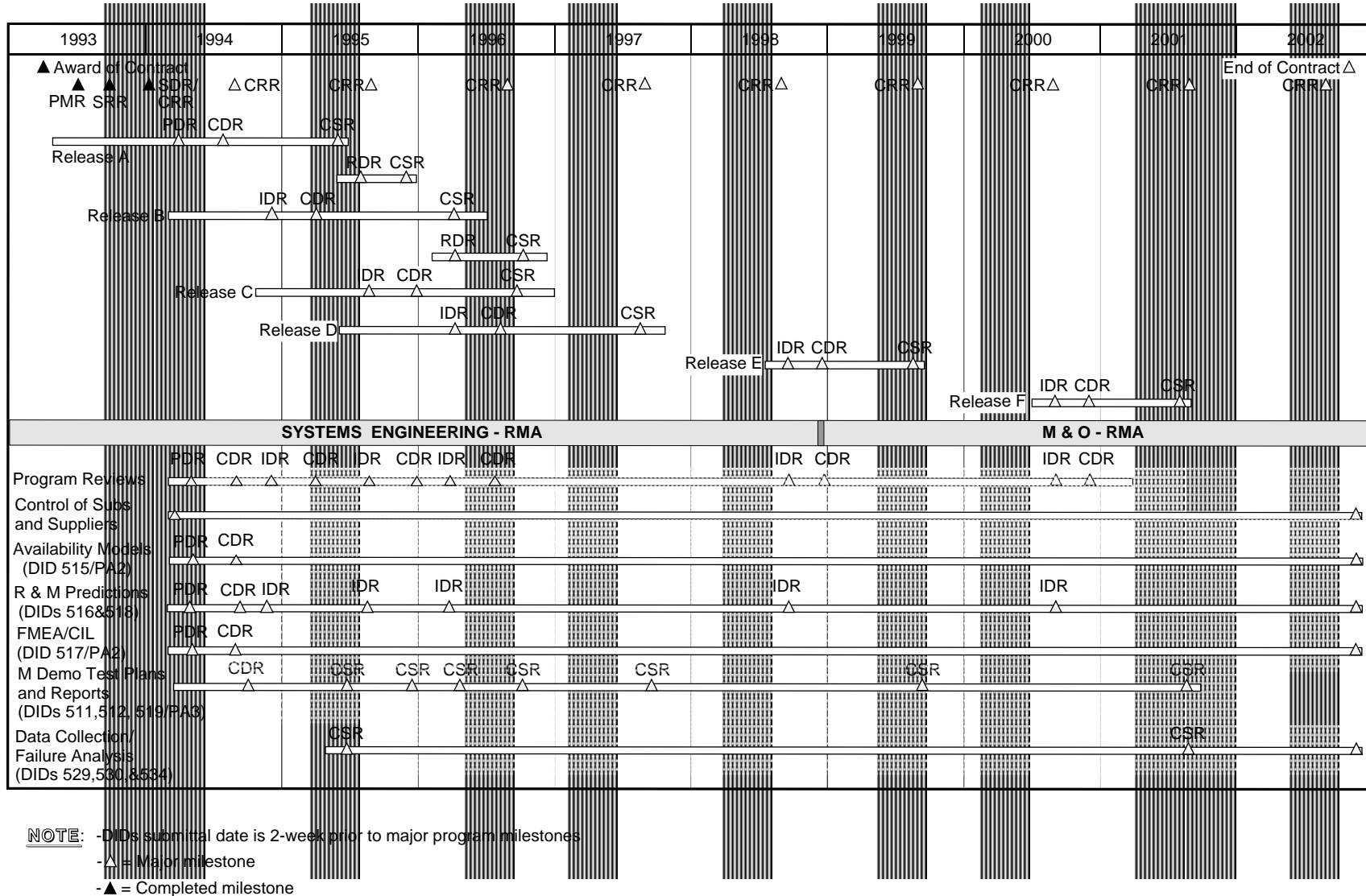
#### 7.1.1 RMA of Government-Furnished Equipment

Government-Furnished Equipment (GFE) hardware, when identified for use, is subject to the same design criteria as other COTS hardware. All RMA data is requested from the Government and evaluated for compliance with ECS standards. Prior to selection for use by ECS, all GFE hardware must meet the ECS RMA specifications. Where the RMA evaluation of the GFE indicates a departure from the ECS RMA requirements, the EOS Project Office is promptly notified in writing. All GFE usage is terminated until formal direction is received from the EOS Project Office.

#### 7.1.2 Program Reviews

All program reviews are supported by ECS RMA engineers as required. As a minimum, all RMA analysis is presented at PDR, CDR, and the IDRs. ECS RMA engineers support GSFC meetings and informal reviews as required.

The process described in Reliability Program Reviews, ECS Project Instruction (PI RM-1-001), is followed in performing this task. This process provides instructions and quality checkpoints to ensure that contractual requirements have been adequately covered at all design and program reviews.



### **7.1.3 Failure Review Board**

ECS RMA engineers conduct the Failure Review Board (FRB) as required. Membership includes representatives from systems engineering, the release or segment organizations, quality assurance, subcontractors, management, and other groups as required. The FRB evaluates hardware and software failures that exhibit a failure rate greater than predicted or are a criticality 1 or 2 failure. Criticality classification is defined in FMEA/Critical Items List (PI RM-1-006). The FRB assigns action items to the responsible organization(s)/person(s) with due dates for defining the corrective action and implementation.

### **7.1.4 Control of Subcontractors and Suppliers**

The ECS program is a team effort; therefore, all requirements of the specification are levied on all team members. HAIS has the lead responsibility to ensure all requirements from the ECS specification are met. Each team member has a negotiated SOW with HAIS that defines specific responsibilities. These agreements allow for a continuous review and evaluation of all team members as well as affording GSFC the opportunity to review and evaluate the ECS team at one location.

Suppliers to the ECS program are selected for the specific COTS product they provide. The selection process starts with a Request for Proposal (RFP) being released. The RFP states specific functional and performance requirements that the COTS product must meet to ensure that the overall requirements of the ECS are met. Documentation requirements are outlined by the RFP and include, at a minimum, RMA data, interface control documentation, and performance assurance conformance data. RMA data is requested down to the Line Replaceable Unit (LRU) level. The LRU is defined by the Logistics Support Analysis (LSA) and vendor recommendations. Each response received for the RFP is evaluated for technical compliance, including RMA and cost. The selected suppliers are issued a contract to supply the COTS product along with all requested data. Control of COTS Subcontractors and Suppliers (PI RM-1-002) discusses this function.

### **7.1.5 Common Use Data Base**

All RMA data is maintained in the Technical Management Data Base (TMDB). This is a common use data base that is used across the ECS program. The RMA data in the TMDB supports LSA requirements and includes COTS vendor RMA data, RMA predictions, and RMA calculations based on observed operational data. The TMDB structure is described in the ECS Systems Engineering Plan (DID 201/SE1) with inputs from RMA engineering.

## **7.2 Reliability Analysis**

The goal of reliability analysis is to ensure that the ECS system meets the  $A_0$  requirements. Reliability analysis is performed concurrently with the design effort and is coordinated with all maintainability tasks. Trade studies are conducted to identify design deficiencies early in the lifecycle, provide tradeoffs between redundancy and maintenance concepts, and provide corrective action recommendations as required.

### **7.2.1 System Availability Modeling**

RMA engineering develops a set of  $A_0$  mathematical models that represent the various ECS strings as defined in the ECS specification. The model is described in greater detail in Availability Models (DID 515/PA2). To accomplish this task, block diagrams are developed for each required functional string. The inputs to the models are the predicted Mean Time Between Maintenance (MTBM) and Mean Down Time (MDT). The reliability data provided by the COTS suppliers is in the form of Mean Time Between Failures (MTBF), which is one portion of the MTBM calculation. The second portion of the MTBM calculation is preventive maintenance data. This vendor-received data is reviewed for completeness, consistency, credibility, and accuracy prior to being used.

The process described in System Availability Modeling (PI RM-1-003) is followed in performing this task. This process provides instructions and quality checkpoints to ensure that all ECS strings have been modeled and the results are certified.

### **7.2.2 Reliability Predictions**

Reliability predictions, developed early in the ECS design phase, are used to validate the allocated MTBM requirements and support the availability modeling activity. Reliability predictions are obtained from the COTS vendors or are determined from comparable data for like items using similar technology in a similar environment. Where acceptable data is not available from COTS suppliers or the hardware is custom, Appendix A of Reliability Prediction of Electronic Equipment, MIL-HDBK-217F will be used to perform the prediction. The reliability predictions will be documented in the Reliability Predictions (DID 516).

The process described in the Reliability Predictions (PI RM-1-004) is followed in performing this task. This process provides quality checkpoints to ensure that all ECS hardware has a valid reliability prediction.

### **7.2.3 Reliability Allocations**

The allocation process is performed early in the ECS design lifecycle in conjunction with the maintainability allocation process. The objective of the allocation process is to ensure that the ECS availability is maximized. The initial allocated values have been derived from similar hardware that was used on other programs. As vendor-supplied data is obtained, the allocations are adjusted accordingly. The process allocates the lowest failure rates to the highest repair rates. The results of the allocation process are used in the Availability Models (DID 515/PA2).

The process described in Reliability Allocations (PI RM-1-005) is followed in performing this task. This process provides quality checkpoints to ensure that all ECS  $A_0$  results are optimized.

### **7.2.4 Failure Modes and Effects Analysis and Critical Items List**

FMEA is performed to identify potential catastrophic and critical failure in the command and control systems of the FOS. The output of the FMEA is a listing of all failure modes, their effects to the next higher assembly, each mode's criticality, and the detection method. This analysis is performed from the LRU level up. The process starts early in the design lifecycle and continues

through the lifecycle of the program. The FMEA (PI RM-1-006) has been developed to follow “Failure Modes and Effects Analysis Procedures for Unmanned Spacecraft and Instruments”, GSFC S-302-89-01. The results of the FMEA and CIL are documented in Failure Modes and Effects Analysis and Critical Items List (DID 517/PA2).

The process described in FMEA/Critical Items List (PI RM-1-006) is followed in performing this task. This process provides quality checkpoints to ensure that the FMEA and Critical Items List (CIL) have been completed in accordance with the SOW and the PAR.

## **7.3 Maintainability Analysis**

The maintainability program is conducted concurrently with the reliability program as part of the system engineering process. Maintainability engineering tasks focus on ensuring specified MDT requirements of the segment strings are met. Design trades are performed to ensure that the A<sub>O</sub> requirements are met. The maintainability program influences the maintenance concept, Maintenance Plan (DID 613/OP1), and provides rationale for LRU spares.

### **7.3.1 Maintainability Predictions**

Maintainability predictions consist of two components: Mean Time To Repair (MTTR) and MDT. MTTR data is provided by the COTS vendors. This data is reviewed for completeness, credibility, accuracy, and consistency with industry standards or comparable data from other vendors. The maintainability demonstration process can verify these predictions. Where data is not available from the COTS supplier, MTTR predictions are made in accordance with MIL-HDBK-472, Procedure II. The MDT is predicted by using the maintenance concept, automatic failover techniques, manual switching of redundant hardware, and the physical design. The maintainability predictions are documented in Maintainability Predictions (DID 518/PA3).

The process described in Maintainability Predictions (PI RM-1-007) is followed in performing this task. This process provides quality checkpoints to ensure that all ECS hardware has a valid MTTR and MDT predictions as required.

### **7.3.2 Maintainability Allocations**

The allocation process is performed early in the ECS design lifecycle in conjunction with the availability allocation process. The object of the allocation process is to ensure that the ECS availability is maximized. The process allocates the lowest failure rates to the highest repair rates. The results of the allocation process are used in the Availability Models (DID 515/PA2).

The process described in Maintainability Allocations (PI RM-1-008) is followed in performing this task. This process provides quality checkpoints to ensure that all ECS A<sub>O</sub> results are optimized.

### **7.3.3 FMEA Maintainability Information**

The Failure Modes and Effects Analysis and Critical Items List (DID 517/PA2) provides the failure modes and the fault detection methods. The information from the FMEA is used to identify and correct design deficiencies. Integrated Logistics Support (ILS) engineers use the

FMEA results to develop the detailed maintenance plan; see Integrated Logistics Support Plan (DID 616/OP2) and Logistics Support Analysis Plan (DID 617/OP3). This task ensures that the ECS remains supportable at the lowest LCC through the 15 year lifecycle.

#### **7.3.4 Maintainability Design Criteria and Operating Standards**

The criteria is developed as part of the RMA program in accordance with Maintainability Design Criteria (PI RM-1-009). The use of the design criteria as a standard facilitates meeting maintainability requirements and ensures support of the ECS through the 15-year lifecycle. Maintainability design criteria includes, at a minimum, the following items: accessibility, human factors considerations, inter-rack cable dressing and identification, identification of external cables, and emergency power-shut-off.

The operating standards of the design criteria ensure that access to the ECS equipment is controlled. Maintenance logs are kept to provide traceability to equipment access and maintenance operations.

#### **7.3.5 Data Collection, Analysis, and Corrective Action System**

A data collection, analysis, and corrective action system is developed for use on the ECS program. This system collects malfunction data and maintenance actions on ECS hardware failures to the LRU level. The data collected is used to verify, update, and augment the RMA prediction data provided earlier in the design process. This system provides the primary data analysis for all failures and maintenance actions to detect design problems and initiate corrective action. The results of the analysis are converted to actual MTBM, MDT, and MTTR. This data becomes part of the common use database discussed in Section 7.1.5.

The process described in the RMA Data Collection System (PI RM-1-010) is followed in performing this task. This process provides quality checkpoints to ensure that all ECS failure data and maintenance actions are collected and analyzed and that deficiencies are corrected.

#### **7.3.6 Maintainability Demonstration**

The maintainability demonstration is planned and conducted using the Maintainability Program for Systems and Equipment, MIL-STD-470, Task 301 as a guide. The demonstration of on-site maintenance is limited to Maintainability/Verification/ Demonstration/Evaluation, MIL-STD-471, Phase II. Test Method 9 of MIL-STD-471 is used as a guide for planning and conducting demonstrations. The selection of faults to be demonstrated come primarily from the FOS critical real-time system functions.

The demonstration verifies the predicted maintainability requirements that validate the specification requirements. Fault detection and isolation methods are evaluated during the demonstration. The maintainability demonstration is performed in accordance with the Maintainability Demonstration Plan (DID 511/PA1). Specific test plans are submitted in accordance with the Maintainability Demonstration Test Plan (DID 512/PA2). The results of the maintainability demonstration are documented in the Maintainability Demonstration Report (DID 519/PA3).

## **7.4 Logistics Support Analysis**

The goal of the RMA program is to ensure that the ECS is reliable, supportable, and has a low LCC. To ensure that these items are satisfied, the results of the RMA analysis become part of the LSA. Logistics Support Analysis (PI RM-1-011) discusses the process to provide the information to ILS engineering. Trade studies are performed to evaluate the proposed designs to determine the most cost-effective maintenance concept.

This page intentionally left blank.

## 8. Software

---

### 8.1 Software Quality Assurance

A description of the software to be developed under the ECS project is found in the Functional and Performance Requirements Specification (424-41-02). The software quality assurance activity, which ensures the quality of that software, is a key function of the Quality Office as illustrated in Figure 3-3, Quality Office Organization. Section 3.1 and 3.2, Figure 3-2, and Figure 3-3 of this Plan describe the management structure and the defined responsibilities of the Quality Office and the QO relationship to the development activities. The Software Development Plan (DID 308/DV2) describes the methodologies the ECS Project Team will use to develop and document the ECS software. The plan, together with the relevant software development Project Instructions also provides a systematic approach to software development through all phases. The Quality Office will verify through in process audits that the software development process is in compliance with the plan and PIs which will include:

- Validating all software and documentation deliverables
- Verifying software engineering and coding standards are followed through code reviews and inspections
- Monitoring and witnessing of testing

In addition, the Quality Office audits the software CM and data management processes to ensure adherence to the methodology outlined in the Software Development Plan (DID 308/DV2) and described in the Configuration Management Plan for the ECS Project (194-102-MG1-001). Procedures to audit the software development activity will be developed based on the methods and techniques described in this plan. These procedures may be found in Contractor's Practices and Procedures Referenced in the PAIP (DID 502/PA1).

#### 8.1.1 Standards

ECS standards are documented in the ECS Standards and Procedures (DID 202/SE1) and in the Software Development Plan (DID 308/DV2). The ECS Project Team will review any standard product software provided by EOS Principal Investigators and Facility Instrument (FI) Investigation Teams to ensure that it complies with standards established by the Science Data Processing Software. The ECS Project Team will comply with these standards for the ECS project. Deviations will be brought to the attention of ECS Project Management. The Quality Office will conduct audits to ensure that these standards are being complied with.

#### 8.1.2 Assurance Function

The ECS project approach to ensuring that all software meets the performance assurance requirements for ECS is managed in two ways. First, the process and procedures for software development are documented in the Software Development Plan (DID 308/DV2) and PIs.

Second, the Quality Office provides an independent monitoring function that assures that software development procedures have been met. The ECS project will employ a software development and quality program relevant to the category of software throughout the system development lifecycle. This program is described in the Software Development Plan (DID 308/DV2) and in Section 3 of this document applies to the four categories of software: heritage, COTS, newly developed and prototyping software. In the case of prototype software the QA activity does not start until this software is declared useful and is turned configuration control. In addition the requirements of Section 6.1 items a through g may also be traced to DID 308/DV2. Table 8-1 QA Planning establishes the QA levels for each type of s/w proposed for use on ECS.

**Table 8-1. QA Planning**

	<b>Audit</b>	<b>Inspect</b>	<b>Test</b>	<b>V&amp;V</b>	<b>RMA</b>	<b>NRCA</b>	<b>CM</b>	<b>Rec. Inspect.</b>
COTS		X	X	X		X	X	X
Newly developed	X	X	X	X	X	X	X	
Prototype		X	X	X	X	X	X	
Heritage		X	X	X	X	X	X	

### 8.1.3 Documentation

The ECS software documentation and related delivery schedules are described in the ECS Project Management Plan (DID 101/MG1). Specific documentation and configuration baseline milestones for software segments are identified by ECS lifecycle phase in Table 8-2, Software Documentation and Configuration Milestones.

### 8.1.4 Science Software Quality Assurance

Algorithm code, delivered to the ECS project from the science community, is required to be the operational software. The following activities are performed against algorithms:

- Evaluation of the delivered algorithm for compatibility with the ECS environment
- Integration with the operational DAAC software interfaces, which involves replacing the Science Computing Facility (SCF) versions of the Product Generation System (PGS) Toolkit in the delivered versions with the DAAC versions
- Development of additional system tests to fully test the algorithm in the PGS environment
- Acceptance testing
- Documentation of the operations procedures for the production algorithm

Problems encountered involving the modification of the algorithm source code in any of the Product Generation Executables (PGEs) are returned to the algorithm development team for modification.

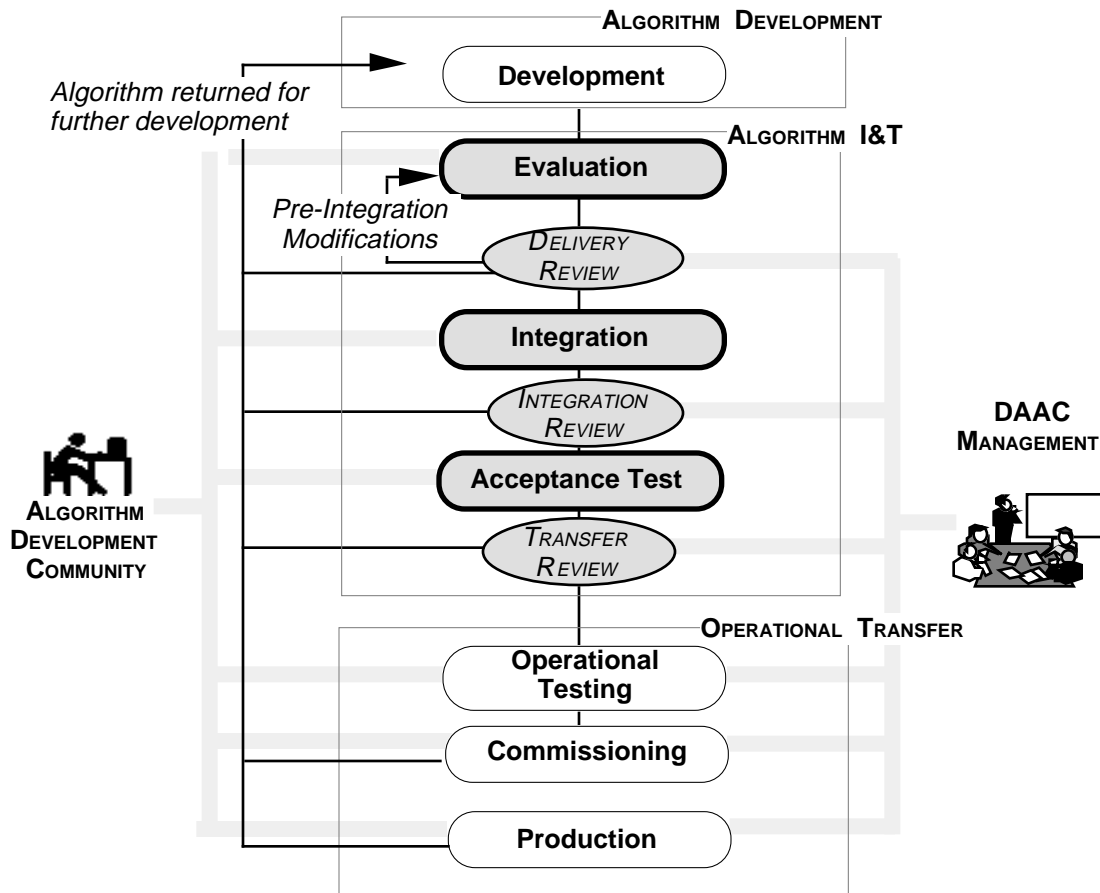
The algorithm activities involve three distinct phases with reviews completing each phase as shown in Figure 8-1, Algorithm I&T Procedure. The phases are Evaluation, Integration, and Acceptance Testing.

The Evaluation phase reviews the delivered algorithm and verifies compatibility with the ECS environment. If incompatibilities are identified, the I&T process will be halted. This phase is concluded with the delivery phase, which provides an initial assessment of the algorithm's suitability for acceptance testing and operational transfer. The goal is to identify the adequacy and completeness of the algorithms at an early stage to ensure efficient use of integration time.

At the Integration phase, the algorithm, having been accepted as suitable, is integrated into the ECS. This phase is concluded with the Integration Review.

The acceptance test phase is carried out according to the acceptance test plan approved at the Integration Review. The phase is concluded with the Testing Review.

Through algorithm development documentation, the Quality Office will verify that the Algorithm Integration Test (AIT) process has been completed. This task will be accomplished through review of provided documentation to verify that the process meets the requirements of the Science User's Guide and Operations Procedures Handbook (DID 205/SE1).



**Figure 8-1. Algorithm I&T Procedure**

### 8.1.5 Software Requirements and Design, Assurance

Upon completion of the Systems Analysis phase of the ECS project and the establishment of the original functional baseline, all requirements, links, and interfaces were entered into the Requirements Traceability Matrix (RTM). RTM is a COTS tool and is the primary tool for maintaining, tracking, and control for all requirements and interfaces. The RTM tool and tool change process are described in the RTM Database Standards and Procedures PI (SE-1-004).

Requirements change authority resides within the ECS Change Control Board (CCB). The CCB and the formal change control and approval process is described in the Configuration Management Plan for the ECS Project (194-102MG1-001).

The Quality Office conducts on-going periodic audits of the RTM. These audits concentrate on the validity and implementation of CCR data. These audits are conducted as per the RTM Project Instruction (SE-1-004).

A brief overview of the software assurance function is contained in the PAIP the Software Development Plan for the ECS Project (308-CD-001-005) and detailed in the PAIP and in the referenced Project Instructions.

During the design stage of ECS software, periodic design inspections are conducted. The inspection process is described in PI SD-1-004. The Quality Office monitors these inspections and collects appropriate metrics as per the ECS Project Metrics Process PI (QO-1-014). Periodically the results of these inspections are reviewed and reported.

## **8.2 Critical Software Items Analysis**

During the ECS design phases, the ECS Project Team will perform an analyses to identify critical software items based on the requirements and design, addressing these items in system architecture, software design, and system testing. The design will address possible failure modes and mitigate the associated risks as determined by the analysis.

Candidate areas for this analysis for the FOS include spacecraft commanding, command authorization, critical command identification, command verification, spacecraft software loads, and load verification. Candidate areas of analysis for communications include data quality checking, processing of data relative to the associated data quality level, and alternate communication paths both internal and external. Based on experience with other satellite control centers and data processing systems, system redundancy, failure capability, fault tolerant systems, and operational procedures will be investigated for risk mitigation approaches in addressing the critical software items.

## **8.3 Software Configuration Management**

The overall ECS CM process is defined in the ECS Configuration Management Plan (DID 102/MG1), and Configuration Management project instructions. The software CM process is outlined in the Software Development Plan (DID 308/DV2) and defined in the Configuration Development Handbook (CM-1-025) and in the CM Build Process PI (CM -1-023).

The ECS Configuration Management Plan (DID 102/MG1) identifies the products included in each software baseline, when each baseline is established, who maintains approval responsibilities of each baseline, and how each baseline change control process is managed. The plan includes a change classification and impact assessment process. The plan, together with the Configuration Management project instructions provide implementing details for the ECS Configuration Management Plan. In addition, the Software Development Plan defines the software CM process for subsystems/release. The Quality Office will audit CM activities to ensure compliance with the above referenced documents. Audit reports will be made available to the GSFC Performance Assurance Office (Code 300).

## 8.4 Nonconformance Reporting and Corrective Action

The Software NRCA process is defined in Project Instruction SD-1-014. The hardware NRCS system will be defined and documented. The NRCA system is used to control and track discrepancies identified in documentation, software, and hardware. For hardware a Malfunction/failure Report (MR) is used for any departure from design, performance, testing, or handling requirement that affects hardware. MRs are defined in Malfunction/Failure Reports (MRs) (DID 529/PA3). Section 9, Hardware Quality, describes this reporting process in further detail.

Nonconformance reporting is initiated against software or a document after they have been placed under configuration control. During the software development I&T phase, identification, resolution, and management of software discrepancies, internal to the corrective action process, will continue to be applied at the beginning of I&T activity for each release between CDR and TRR. Any individual associated with the ECS program who detects a discrepancy, can initiate a nonconformance report (NCR) as per the NRCA PI SD-1-014. The segment/release managers are responsible for assigning a technical lead to investigate the problem. NCRs will be entered into the NRCA Distributed Data Tracking system (DDTs™). DDTs™ is a COTs tool that has been customized to meet ECS requirements. If a correction to software is required, the software CM process is used to implement and control the change. The software CM process is outlined in the Software Development Plan (DID 308/DV2) and defined in the Configuration Development Handbook (CM-1-025). All of the organizations involved in the test program, including the Quality Office, participate as members of the CCB. When changes require CCB approval, the Quality Office reviews all nonconformance reports, prior to CCB submission and CCB closure, to ensure that all required actions have been completed. Software nonconformance reports will be identified in detail in Software Nonconformance Reports (DID521/PA3) and in summary form in the Performance Assurance Status Report (DID 503/PA3).

The NRCA Distributed Defect Tracking (DDTs™) system includes, but is not limited to the following data items:

- Unique identification number (automatically assigned by DDTs™)
- Software product identification including Segment and subsystem
- Source of error (hardware, software, documentation, etc.)
- Originator and Origination date
- Brief title
- Summary description of the discrepancy
- Status
- Test case (where error was detected)
- Severity level
- Proposed corrective action
- Corrective action taken

- Version identification of the corrected product
- Date of the correction
- Test verification
- Closure date
- Related CCRs

## 8.5 Security

ECS security is comprised of the following components: Automated Data Processing Equipment (ADPD), communications, personnel, and physical security. The LSMs provide authentication and authorization services which control access to ECS services and data, based on security policies received from ESDIS and managed at the System Management Center (SMC). The LSMs receive overall security policies from the SMS, and are responsible for its implementation in their administrative domain, which is their DAAC. Physical security will be in place to protect ECS personnel and control access to the ECS system hardware, software, and data. Security Engineering tasks will be discussed in greater detail in the ECS Security Plan (DID 214/SE1). A Security-Sensitive Items List (DID 514/PA2) will list the software and hardware items that are sensitive to loss, tampering, or misuse that will result in potential damage to the ECS functions. For each type of interface that can occur, its impact and planned security control will be provided. The Quality Office will audit the SMC for compliance with the ECS Security Plan. Audit reports will be made available to the GSFC Performance Assurance Office.

## 8.6 Software Design and Implementation Process

The developed software design and implementation process for the Project is defined in Section 4.1 and 4.2 of the Software Development Plan (308-CD-001005). Section 4.1 describes in an overview fashion the System Design, incorporation of “Design Derived” requirements, design synchronization across release and capture of lessons learned.

Section 4.2 describes the software development process including preliminary and detailed design and the design implementation. Further design and implementation process detail is provided by the following project instructions.

SD-1-004	Software Inspection Process
SD-1-006	Common Software Development Guidelines
SD-1-007	Coding Standards for FORTRAN
SD-1-008	Coding Standards for Ada
SD-1-009	Coding Standards for C
SD-1-010	Coding Standards for C++
SD-1-011	ECS Program Design Language (PDL) Guidelines
SD-1-012	Heritage Software Selection Guidelines

SD-1-014          Software Nonconformance Reporting and Corrective Action System  
process

SD-1-015          Software Naming Conventions

When the coding phase of the process is completed for any release, that release enters the Integration and Test phase. This and subsequent phases, as described in this document, verifies the implementation of the design.

## 9. Hardware

---

### 9.1 Hardware Quality Assurance

The COTS hardware QA program provides a solid foundation for establishing and controlling the quality of vendor products used within the ECS. All hardware for ECS will be COTS, with no custom hardware development anticipated. However, in the event that it later becomes necessary to develop custom hardware, the applicable requirements of the ECS PAR will be complied with, as discussed in 9.10.1. For more detail on what assurance activities will be administered to COTS, Heritage and previously developed hardware and software refer to Section 3 of the PAIP.

This section describes the performance assurance activities used to ensure the product compliance of COTS computer hardware for the ECS. The ECS Project Team is responsible for commercial hardware QA.

- Provide the NASA with equipment having "zero defects"
- Monitor the procurement process for contract conformance and compliance with ECS standards and objectives
- Ensure that NASA has reliable, available, and operable equipment that performs as required

In addition the program will:

- Demonstrate recognition of the quality aspects of the contract and the importance of using an organized approach to achieve them
- Ensure that quality requirements are identified, established, and satisfied throughout all phases of contract performance, including design, development, fabrication, processing, assembly, inspection, test, packaging, shipping, storage, maintenance, and mission use, as applicable
- Provide for the detection of actual or potential deficiencies, system incompatibility, marginal quality, and trends or conditions which could result in unsatisfactory quality
- Provide timely and effective remedial and preventive action

The status of the Quality Program will be in accordance with paragraph 1.6 of the PAR.

An overview of hardware QA follows:

- The hardware QA process begins when the product specifications are forwarded to vendors for competitive bid. The Procurement Management Plan (DID 110/MG2) and COTS Vendor and Supplier Quality (PI QO-1-012) discuss the key vendor and product criteria considered in source selection. Product specifications include the applicable reliability and maintainability required of the product and the functional and performance specifications (including open-architecture and vendor-independence standards).

- Equipment receiving inspections are performed to verify that all unit products conform to specification and contract requirements. This process is described in the COTS Unit Receiving, Inspection and Verification Instruction (PI QO-1-013).
- A document trail is maintained and controlled by various CCBs. Engineering Change Proposals (ECPs) and Configuration Change Requests (CCRs) are documented, reviewed, and approved before implementation. Configuration control is maintained to control changes and provide a traceable path to the previous configuration and a baseline. This process is described in the Management Plan (DID 102/MG1) and the Property Management Plan (DID 602/OP1).
- Each product is identified by a unique part or type number, consistent with the ECS Configuration Management Plan (DID 102/MG1) and the Property Management Plan (DID 602/OP1). This information is recorded in a permanent, accessible database that enables the COTS Hardware Procurement, CM and ILS Property Management teams to track the product from receiving throughout its lifecycle. This database is Vendor Costing and Tracking System (VCATS).
- A closed-loop nonconformance control system is maintained to track specific LRUs, equipment, or products that malfunction and/or contain discrepancies. This type of control system allows nonconforming products to be identified, documented, tracked, and disposition in a structured, auditable process. A PI identified as Nonconformance Reporting Corrective Action (NRCA) system (document not yet written) will describe this process.
- A complete maintenance and operating history of baselined ECS COTS hardware will be kept in operations. Configuration logs will be maintained with the equipment. Logs are maintained in the SMC systems supporting Maintenance, CM, and Operations (see Section 9.16) This data is used for RMA validation and analysis and consists of all corrective maintenance, preventive maintenance, operations, and engineering changes.
- Configurations are identified and documented according to the ECS Configuration for ILS support.
- Product integrity is maintained during shipping, handling, and storage. Environmental and packaging requirements are followed to prevent damage and are discussed in the COTS Unit Receiving, Inspection, and Verification Instruction (PI QO-1-013).
- Established inspection and test procedures from the Applicable Documents List (section 2.2) are followed throughout the ECS lifecycle from procurement receiving inspection to acceptance testing. These procedures validate compliance with contract, performance, and design requirements; identify and document nonconformances early; and contribute to ECS system quality.
- Training is provided for personnel responsible for performance assurance, operations, and maintenance actions. This training is in accordance with the ECS Training Plan (DID 622/OP2) and applicable specifications and certifications necessary to perform inspection/test or maintenance activities. Training status records are maintained for all personnel. All training programs and records are available for examination by the Government.

## **9.2 Quality Assurance Plan**

This section of the PAIP describes the tasks to be performed in the implementation of Section 7 of the PAR, applicable to COTS hardware, new hardware, and to the integration, test, maintenance, and operation of the ECS. QA actions appropriate to the ECS Maintenance Plan (DID 613/OP1), the ECS Operations Plan (DID 608/OP3), and the ECS Maintenance and Operations Management Plan (DID 601/OP1) are described.

## **9.3 Document Change Control**

CCBs will be formed as defined in the ECS Configuration Management Plan (DID 102/MG1). Members are identified to participate in each of these CCBs. The responsibilities and activities of these boards are defined to include reviewing ECPs and CCRs. Changes to baselined documents will be made through a CCR or ECP, as appropriate.

Configuration Status Accounting is performed, enforced, and verified to ensure that the current status of the configuration is documented. Historical records are maintained to provide a traceable path to previous configurations.

QA Personnel will ensure that documents and revisions are controlled in accordance with the Earth Observing System Configuration Management Plan GSFC 420-20-02 and that evidence shall be provided of compliance with the as-built documentation as a basis for acceptance.

## **9.4 Identification and Traceability Requirements**

ECS Configuration Status Accounting (CSA), under the ECS Configuration Management Plan (DID 102/MG1) and the Property Management Plan (DID 602/OP1), utilizes a product identification and tracking system (VCATS). Each product is identified by a unique part or type number. The Equipment Identification Number (EIN). Where control of individual products or product lots is required, date codes, lot numbers, serial numbers, or other identification are used as appropriate. After receiving and verification of equipment, the ILS team will update the Property Master Index (VCATS) database before releasing it for installation or storage. COTS hardware is traceable initially to the unit level and serial number, of items that qualify under Property Management as EINs. After any maintenance activity, traceability is expanded to the replaced LRU level. For LRUs that are stocked as spares, initially all like articles are traceable (including those installed in the higher level assembly). Tracking begins upon receipt of the equipment, by the ILS team, at the receiving inspection where the equipment will be bar coded with the unique EIN.

## **9.5 Procurement Requirements**

Applicable QA procurement requirements defined in COTS procurement documents are:

- Product change, age control and limited-life products, Inspection and Test records, Government Source Inspection (GSI), contractor source inspection, and resubmitting of nonconforming material.

### **9.5.1 Product Changes**

Applicable product changes, such as changes in design, and changes that may affect the quality or intended end use of the item, are submitted for processing in accordance with the CM change control procedures. If a proprietary item is procured, those changes are also submitted for processing; however, the ECS Project Team does not anticipate procuring proprietary items.

### **9.5.2 Age Control and Limited-Life Products**

As specific products with age control and limited-life restrictions are identified, the COTS hardware team determines the detailed control, inventory, storage, and issue procedures for each product. This is based on product information and the specifications and requirements that led to the selection of that item for procurement. The Property Management Plan DID602, and MCO Procedures to be developed DID609 describe the process.

### **9.5.3 Inspection and Test Records**

Vendor testing results and equipment inspection and test records are maintained by the vendors for procured COTS hardware items. ECS Procurement documents specify what records the vendor must supply with the deliverable item. These documents are retained as quality records. COTS Vendor and Supplier Quality PI (QO-1-012) describes this process.

### **9.5.4 Government Source Inspection**

Upon request, ECS will arrange with vendors to give Government representatives access to production line, QA operations, and QA personnel. When the Government elects to perform a GSI at a supplier's plant, the following statement will be included in the procurement document:

“All work on this order is subject to inspection and test by the Government at any time and place. The Government quality representative who has been delegated NASA quality assurance functions on this procurement shall be notified immediately upon receipt of this order. The Government representative shall also be notified 48 hours in advance of the time that articles or materials are ready for inspection or test.”

The Procurement Management Plan DID110 describes the process within which the government representative makes a GSI determination.

### **9.5.5 Procurements Not Requiring Government Source Inspection**

Procurements that do not require GSI will include a statement to the effect that “the government has the right to inspect any or all of the work included in this order at the supplier's plant”. The government maintains the right to verify COTS product quality.

### **9.5.6 Contractor QA Activity at Source**

When ECS QA activity is required at a supplier's plant, the procurement document will so indicate.

### **9.5.7 Resubmitting of Nonconforming Articles or Materials**

All equipment that has been returned to vendors for nonconformance, and later resubmitted, is re-inspected and tested. Only after successfully passing inspection and testing is the equipment released from receiving and inspection. It then carries a history of its original nonconformance and resubmission.

## **9.6 Review and Approval of Procurement Documents**

The foundation of the COTS QA process is the selection of products and vendors known for their quality, performance, and the verification that these products comply with procurement and performance specifications. QA personnel assist in developing, reviewing, and approving the RFP documents for COTS products before their release to ensure that applicable QA requirements are included. The ECS COTS procurement process is explained in Section 6 of the Procurement Management Plan (DID 110/MG2). Evaluations, reviews, and approvals occur early and throughout the process, including Government approvals when appropriate.

## **9.7 Procurement Review by the Government**

Procurement documents are provided to the Hughes Management Operations Office to review for compliance with contract requirements, and to forward for Government approval. The onsite Quality Assurance representative (DCMAO QAR) also reviews procurement documents for contract requirements and need for GSI. Source inspection at the vendor's facilities is a right available to the Government and HAIS. Government inspection will not replace contractor source inspection or relieve the contractor of responsibilities for product reliability, quality, and safety.

## **9.8 Contractor Source Inspection**

The ECS Quality Office plans to verify product quality at the EDF or at the NASA site, for product shipped directly there. If any of the following conditions exist, source inspection at the vendor's facilities will be performed:

- In-process, end-item controls, or tests that are destructive in nature prevent verifying quality at the EDF or on site
- It is not feasible or economical to verify quality solely by inspections or tests at the EDF or on site
- Special tests are to be performed by the vendor that are not economical to repeat

## **9.9 Contractor Receiving Inspection**

The COTS ILS team performs a receiving inspection to ensure that all products received conform to specification and contract requirements. The receiving inspection process only releases acceptable conforming product and holds non conforming product for vendor warranty disposition. The vendors will maintain inspection and test records as evidence of their inspection program. The procurement documentation specifies test records and data that are to be provided

with the deliverable item. As outlined in COTS Unit Receiving Inspection and Verification (PI QO-1-013), all vendor deliveries are inspected for conformance to purchase documents and requirements and any shipping damage. Both the Property inspection and Procurement teams act immediately on nonconformances found and segregate the product for vendor warranty disposition.

Experienced computer systems technicians complete the installation of most ECS COTS products. For products that are installed by the manufacturer, such as super computers, installation team leaders monitor the installation to verify that proper procedures for installation and testing are followed by the manufacturer. ECS COTS product technicians who assemble and install ECS hardware follow the manufacturer's installation procedures. This ensures that manufacturer warranties remain in effect and that the equipment will function as designed.

Inspections and tests are conducted in accordance with the COTS Unit Receiving, Inspection, and Verification (PI QO-1-013) on selected product characteristics appropriate to products and technology, to verify their acceptability. Appropriate emphasis is placed on the selection of characteristics that have not been contractor-source inspected and those for which nonconformance is difficult to detect during subsequent inspection and testing. Disassembly is performed for detailed verification and LRU inventory, when appropriate, to the product assembly and configuration.

The assignment of the unique EIN in the property records, and on the equipment through the barcode shows ECS acceptance status. No other marks, stamps, or tags are used to show acceptance status.

Products and their records will however show any non conformance status if circumstances require release from receiving-inspection. They are protected for subsequent handling or storage.

The following tasks are also completed during receipt inspection:

- Inspection and test records are maintained, including copies of documents submitted by the vendor
- Age control and limited-life records are updated or established, as appropriate
- Electrostatic discharge control procedures and environmental control requirements are followed
- Identification and serial numbers are collected for equipment tracking purposes in accordance with the Property Management Plan (DID 602/OP1)

## **9.10 Control of Fabrication, Integration, and Operations Phase Maintenance Activities**

An Integration and Inspection Flow Plan (DID 522/PA2) will be developed in the event ECS designs and fabricates custom hardware. A Maintenance and Operations Management Plan (DID 601/OP1) will describe the management system, controls, functions, policies, procedures, and documentation to be used in fulfilling the M&O requirements of each site. Property

Management and Maintenance controls will ensure that only conforming hardware articles are released and used during integration and operations phase maintenance activities.

### **9.10.1 Fabrication and Inspection Requirements**

Because only COTS hardware is procured for the ECS program, no fabrication activities are planned by the ECS team. Appropriate manufacturing process controls are supplied by the COTS vendor, as part of their QA Program. As described in the Procurement Management Plan (DID 110/MG2) and the COTS Vendor and Supplier Quality (PI QO-1-012), the vendor selection process considers vendor and product history, performance, reliability, supportability, and commercial market experience and success. This process may select an established COTS product line that requires no additional inspection requirements, or it may select a higher risk COTS new technology/product line that should be evaluated within the context of vendor product and quality history, as well as ECS program and technology risk management. New technology or product line COTS procurements will be evaluated by the ECS Quality Office and a recommendation on source inspection or additional quality actions will be made to GSFC Performance Assurance to achieve a joint agreement on appropriate action.

This recommendation will be a plan considering the following PAR requirements that are not applicable to an established COTS product:

- Subcontractor and supplier audits
- Contractor source inspection
- Inspection and test points
- Manufacturing process specifications and procedures
- Drawing change control
- NHB workmanship standards for fabrication
- Training and certification of personnel to the NHB workmanship standards
- MRB activities

The Integration and Inspection Flow Plan (DID 522/PA2), Contractors Workmanship Procedures (DID 523), and various Project Instructions may be affected by this planning. ECS hardware maintenance procedures will be described in the Maintenance Plan (DID 613/OP1) and the Maintenance and Operations Management Plan (DID 601/OP1).

In the event that it later becomes necessary to design and/or build custom hardware, applicable requirements of the ECS PAR will be implemented. The PAIP will be updated as necessary at that time.

### **9.10.2 Training and Certification for Manufacturing, Integration, Inspection, Operations, and Maintenance Personnel**

Training to prepare and certify ECS operations, integration, inspection/test, and maintenance personnel will be developed and implemented in house or from third-party or COTS product

vendors. Consistent with the ECS Training Plan (DID 622/OP2), training will be based upon the functional and technical specifications necessary to perform operations, integration, inspection/test, or maintenance activities. Recertification will be required annually.

Maintenance level training will be consistent with the ECS Maintenance Plan (DID 613/OP1) and include diagnostics, troubleshooting, and fault isolation to the LRU replacement level, but will not include any subsequent LRU level repair. No training or certification in manufacturing processes including soldering, module welding, potting, harness fabrication, encapsulation, etc., is planned, as these processes are inherently part of COTS vendor fabrication or manufacturing. In the event that it later becomes necessary to train personnel in these areas, (see 9.10.1) training and certification will be provided. COTS vendor source selection is based on their standard COTS product compliance with procurement specifications and performance success in the commercial market using commercially acceptable manufacturing processes and quality programs.

Records will be maintained of the training, testing, certification, and recertification status of personnel. All training programs and records will be available to the Government Assurance Representative.

### **9.10.3 Process Evaluation and Control**

COTS hardware will be procured for the ECS program, and no fabrication activities are planned, except as described in 9.10.1. Appropriate manufacturing process controls are supplied by the COTS vendors as part of their QA program.

## **9.11 Electrostatic Discharge Control**

The ECS Maintenance Plan (DID 613/OP1), Environmental Control Plan (DID 532/PA1), and Maintenance and Operations Management Plan (DID 601/OP1) will describe the program to control Electrostatic Discharge. Awareness and prevention practices will be followed in implementing the COTS Unit Receiving, Inspection, and Verification (PI QO-1-013). The program shall include provisions for work area protection, handling procedures, training, intra-plant protection, delivery packaging, and QA verification.

## **9.12 Nonconformance Control**

A closed-loop nonconformance control system for malfunctions and discrepancies is maintained. Nonconforming products are identified and, if practicable, physically isolated for review and disposition action. Provisions are made to control nonconforming products that cannot be isolated. The control system includes the following activities:

- Documentation of each nonconformance traceable to the specific equipment, LRU, material, or product on which it occurred.
- Assignment of a unique and traceable document number for each malfunction and discrepancy. Description of the nonconformance and the required characteristic or design criteria, if applicable.

- Performance and documentation of analyses and examinations to determine the cause.
- Assignment, implementation, and documentation of timely and effective corrective action on the products and applicable documents.
- Segregation and disposition of the nonconforming product and any other products affected.
- Signatures of authorized personnel on the appropriate nonconformance documents.
- Accumulation and use of trend data and the performance and documentation of trend analyses to identify adverse trends.
- Close-out of nonconformance documentation after verifying that effective corrective actions have been taken on the nonconforming articles and any other articles potentially affected.

Hardware Nonconformance discrepancies are described in Section 9.12.1 and malfunctions in Section 9.12.2. Software Nonconformance is discussed in Section 8.6. The Verification Plan for the ECS Project (DID 401/VE1) also discusses discrepancy disposition and resolution in Section 4.3. The NRCA System PI (PI QO-1-009) will describe malfunction reporting responsibilities and procedures interfaces. QA monitors, audits, and ensures the effective operation of the NRCA system.

Reliability engineering and ILS are the principal users of NRCA, performing trend analysis and determining impact and adjustments to RMA predictions, Operational Availability, design, maintenance sparing, etc.

### **9.12.1 Control, Disposition, and Reporting of Discrepancies**

Documentation of discrepancies starts with the receipt of procured product or materials. Each discrepancy is promptly documented. This documentation includes the report number, date, product identification, manufacturer, description of the nonconformance from specification, disposition, and authorized approval signatures.

Each nonconforming product is reviewed by the ECS QA team and, as appropriate, engineering personnel. The product is normally subject to one of the following dispositions:

- Return to the vendor/supplier with nonconformance information, and assistance as necessary, to permit corrective and preventive action and warranty action if applicable.
- Repair in accordance with standard repair procedures. The failed LRU is also promptly repaired and returned to service in accordance with approved maintenance procedures.
- Rework and scrap are dispositions normally applicable in hardware manufacture and fabrication and not planned for use.
- Submit to MRB when above dispositions are not appropriate.

These initial review dispositions are recorded on nonconformance documentation.

The Material Review Board (MRB) is an informal ad hoc board comprised of members from the ECS Quality Office, Engineering, and ILS teams, with a Government Quality representative. The primary responsibility is to decide on the disposition of submitted nonconforming product that will not be routinely dispositioned by return to vendor under warranty. Because COTS hardware with vendor warranties will be procured for ECS instead of designing and fabricating custom hardware, it is not planned to convene the MRB as a standing board. The MRB, if convened, will be tasked with defining procedures for documentation, membership, responsibilities, dispositions, and general operation. MRB responsibilities may be delegated to vendors/suppliers with the approval of NASA or its authorized assurance representative.

### **9.12.2 Control, Reporting, and Disposition of Malfunctions**

A malfunction report is initiated immediately for any departure from performance, design, testing, or handling requirement that may affect the function of the ECS hardware or compromise mission objectives. This includes system-level malfunctions, whether in hardware, software, or both. Reporting begins with the first power application at the lowest level of assembly of an electrical or electronic item or the first operation of a mechanical item, after vendor delivery. Software nonconformance reporting is described in Section 8.6.

The NRCA system and procedures will be described in an ECS PI to be developed (PI-QO-1-009). This includes the operation of a Risk Assessment Rating system based on Impact Ratings and Corrective Action Effectiveness Ratings.

The Impact Rating identifies the impact the problem or malfunction would have on the flight hardware and/or software performance capabilities if it occurred during the mission. There are three levels of rating:

- Catastrophic or major degradation to mission
- Significantly degrading to mission
- Negligible or no impact on mission

The second rating factor Corrective Action Effectiveness Rating shall be assigned a numerical rating which depends on the confidence in understanding both the causes of the incident and the effectiveness of the corrective action. This assessment shall be based on the following criteria:

- a. "A" - Known cause coupled with certainty of the effectiveness of corrective action
- b. "B" - Unknown cause coupled with certainty of the effectiveness of the corrective action
- c. "C" - Known cause coupled with uncertainty of the effectiveness of corrective action
- d. "D" - Unknown cause coupled with uncertainty of the effectiveness of corrective action

A summary of the open nonconformances is submitted as part of the Performance Assurance Status Report (DID 503/PA3). This summary lists each problem or malfunction as a separate line item and provides the identification number and complete identification of the affected product, its use, the environment, date of occurrence, a brief description of the malfunction, its cause, and the corrective action to be taken. Before removing any item from the "open" list, the last summary report shows the corrective actions actually taken and the date closed.

The Failure Review Control FRB is comprised of members from the ECS Quality Office, Engineering, Reliability Engineering, and ILS teams, with a Government Quality Representative. The primary responsibility of this board is to ensure that critical malfunctions (Impact Rating 1 or 2) are investigated, analyzed, and corrected and that their causes are determined. Critical malfunctions are most likely to involve the command and control functions of the FOS or the inability to produce or irretrievable loss of Essential Data Products. The FRB performs trend analysis based on data from the nonconformances and supporting databases. The NRCA system will provide procedures on the operation of this board and the Risk Rating system.

### **9.12.3 Reporting of Spacecraft Orbital Anomalies**

Spacecraft Orbital Anomaly Reports (SOARs) are issued immediately after any anomaly occurs on EOS flight hardware or software during the mission. The Impact Rating system is used to identify the seriousness of the problem. GSFC form for reporting will be used to report SOARs and all project team members are instructed to use this form. The MOM is immediately notified after an anomaly occurs. The NRCA system will contain provisions for tracking SOARs to discrepancy reports where applicable.

## **9.13 Environmental Controls**

The Environmental Control Plan (DID 532/PA1) will establish, document, and implement suitable environmental and cleanliness standards, procedures, and controls for all ECS areas used for the operation, storage, maintenance, repair, inspection, or test of system equipment. The Quality Office monitors the compliance of operations and maintenance activities with this plan.

## **9.14 Special Notices and Alert Information**

If NASA provides the ECS Project Team with any special notice of general problems, or with inquiries about their applicability to the ECS, the ECS Project Team will respond as required by the Government (10 working days after receipt of notice). Included in the response will be any follow-up action, if necessary. The ECS Quality Office coordinates the HAIS response.

The specific Response to Problem Notices and Alerts (DID 533/PA1) and status summaries are included in the Performance Assurance Status Report (DID 503/PA3). If necessary, the Procurement Office, which maintains vendor and product histories, will contact vendors for additional information.

## **9.15 Inspections and Tests**

The Verification Plan (DID 401/VE1), Segment Integration and Test Plan (DID 319/DV1), ECS System Integration and Test Plan (DID 402/VE1), and supporting procedures to be developed describe an inspection and test program that demonstrates that contract and specification requirements are met. The Segment IET Procedures DID 322 and ECS System IET Procedures DID 414 are the supporting procedures.

Throughout the ECS lifecycle various inspection, demonstration, and test activities will occur, beginning with the vendor's QA program, as evidenced by documentation received with the

product. These activities are generally subject to the procedures in the Environmental Control Plan (DID 532/PA1) and appropriate personnel certification requirements in the ECS Training Plan (DID 622/OP2).

### **9.15.1 Planning**

The ECS Maintenance Plan (DID 613/OP1) and the Maintenance and Operations Management Plan (DID 601/OP1) describe the repair and preventive maintenance activities in the ECS operations phase and a documentation system that substantiates their accomplishment. The inspection and test planning function will provide for orderly, timely, sequenced scheduling of activities, effective coordination, approved inspection and test procedures, available calibrated Test Measurement Diagnostic Equipment (TMDE), and coordination of activities conducted by the designated Government Assurance Representative.

### **9.15.2 Inspection and In-Process Test Procedures**

Inspection and test activities will be documented and conducted in accordance with approved procedures physically located at the applicable inspection or test station. All procedures (DID 322, 414, 609) will include, as applicable, the product identification/nomenclature, characteristics to be inspected or tested, accept/reject criteria if applicable, equipment and TMDE needed, standards, safety, and environment.

### **9.15.3 Inspection Activity**

As described in the COTS Unit Receiving Inspection and Verification (PI QO-1-013), vendor Quality documentation received is retained as evidence of in-process inspections. Each LRU and hardware end-item is inspected when received for configuration, visible workmanship, and purchase order compliance, prior to integration into larger configurations. Instructions prepared in advance of the test or inspection are developed based on the requirements of that particular product and function. Nonconformances are promptly documented, processed, and any open items documented and carried forward into the next level. Stored and stocked parts, materials, and spare COTS products are periodically inspected for proper storage, environment, and packaging.

The Maintenance and Operations Environmental Control Plan (DID 532/PA1) will be followed. The amount and frequency of inspections is product dependent.

### **9.15.4 QA Activities During the Integration, Test, and Operations Phases**

QA will ensure that the hardware and software product is integrated, tested, operated, and maintained in accordance with controlling procedures and plans. QA will provide surveillance of all tests, inspections, and operational and maintenance activities by following pre- and post-test assurance activities and ensuring that tests are conducted according to approved specifications and procedures, with accurate and complete recording of data and results.

Before COTS software integration, diagnostics and demonstrations are performed on all equipment to verify proper operation. After installation of COTS, software assurance verifies that the software has been installed, functions correctly, and does not create new system problems.

The integration and testing of software is described in Section 5, Verification Requirements and Section 8, Software Assurance Requirements. This also applies to modified or new software developed in sustaining engineering activity during the operational phase. The same basic QA verification requirements exist for software as they do for hardware. QA will verify that the software product is ready for test, approved test software and documents are present, products are identified and configured, approved specifications and procedures are followed, recording of data and results is accurate and complete, and nonconformances are properly handled.

Throughout the M&O phase, QA will verify that applicable practices and procedures are being implemented and followed.

#### **9.15.5 Records of Inspections and Tests**

Records, including logs, of all inspections and tests will be prepared and maintained to show that all operations have been performed, the objectives met, and the end-item fully verified. These records will be maintained and stored in a readily accessible, identifiable, and retrievable form, and will represent a continuous chronological history of product activity. The Quality Office verifies that the records are complete and are appropriately included in the Acceptance Data Package.

Records shall cover each component, subsystem, and system. As the product is integrated, records of lower level assembly products shall be combined into those for the end item as a means of compiling a continuous, chronological history of identified product, fabrication, assembly, and inspection actions, and tests as well as idle periods (storage), movement of the product, repairs, approvals, maintenance, configuration data, etc.

#### **9.16 Maintenance Records**

As required by the ECS Maintenance Plan (DID 613/OP1) and the Maintenance and Operations Management Plan (DID 601/OP1), operating and maintenance records are kept during the operational phase. This data is used to support the RMA program and to provide logistics data. These records contain at least the following data items:

- Operating logs for each piece of equipment. This data includes on/off times, operating time, downtime for each maintenance/repair event, equipment rack access records (times opened/closed, purpose, and identification of individuals), and malfunction frequency data.
- Configuration logs for each piece of equipment. Data includes a current configuration list for the equipment, dates and times of equipment or LRU installation and removal, and serial numbers of LRUs removed for repair and for the replacement LRUs.
- Maintenance work orders. The system should cover pertinent data, including LRU identification, diagnostic data, repair operations and steps, repair time duration, hardware disposition and routing, spare parts availability (and resupply delays), test procedures for repaired items, test results, etc.

These records are maintained and stored in a readily accessible, identifiable, and retrievable form at the ECS Project Team facility for the duration of the contract. The maintenance records are available for NASA inspection at the ECS operations work sites and maintenance sites.

## **9.17 Configuration Verification**

The Quality Office verifies that the as-built product complies with the as-designed configuration listing for any acceptance activity on system hardware. The ECS Configuration Management Plan (DID 102/MG1) and procedures apply.

## **9.18 Metrology**

Calibration will be maintained and documented on all instruments, tools, gages, fixtures, and equipment used in the test and inspection of ECS hardware, in accordance with the ECS Maintenance Plan (DID 613/OP1), and applicable provisions of Calibration System Requirements (MIL-STD-45662), Calibration intervals are defined and suitable to the equipment stability, accuracy, and purpose. Manufacturer's recommendations are considered. A scheduling system recalls equipment, notifies users, and serves as a calibration history by item. Extensions and delinquencies are monitored and reported on routinely. A certified laboratory or contractor is used with standards accuracy that meets or exceeds the equipment accuracy requirements. Equipment bears visible evidence of calibration status. Vendors or third-party maintenance providers are required to have an equivalent calibration program with visible equipment evidence of current status.

## **9.19 Stamp Control System**

The unique EIN bar code label functions like a stamp and shows that ECS product has undergone source and receiving inspection. Maintenance and Operations procedures to be developed will identify if and when stamps, decals, tags, or seals shall be used to show operational, maintenance, or use restriction status. A formal stamp control system for products or records will not be implemented for the receiving, inspection, verification, integration, testing, operations or maintenance of ECS COTS products. Stamp Control requirements will be appropriately applied in the event of custom hardware manufacture or fabrication.

## **9.20 Handling, Storage, Preservation, Marking, Labeling, Packaging, Packing, and Shipping**

Equipment is examined upon receipt for proper identity, quantity, and any evidence of damage. Items requiring finish protection or environmental controls, or having exposed wires/components sensitive to Electro Static Discharge (ESD), or other handling damage, are enclosed in protective containers as specified by engineering packaging requirements.

Packaging inspection is not required for internal movements (within Hughes buildings). Integrity is maintained by all personnel involved. Item identification, configuration, traceability, and quality status are maintained at all times. The ECS Quality Office maintains surveillance and

observation over actual practices and conducts audit inspections, as necessary, to insure compliance. ESD awareness training is conducted as needed.

Operating, environmental requirements are incorporated into product specifications during the procurement cycle. These are provided to the prospective vendors in the RFP and included in the vendor subcontract. Once the environment and equipment has been identified, control standards for the environment are documented and submitted to the Government as required.

Work areas are required to be clean, appropriately padded or cushioned, and conform to applicable environmental and ESD controls. The majority of the computer and communications LRUs require special handling any time they are outside the manufacturer's protective packaging to prevent damage from electrostatic discharge. The provisions of NHB 6000.1D, "Requirements for Packaging, Handling, Storage and Transportation (PHS&T)," will be used in satisfying the ECS requirements.

## **9.21 Government Property Control**

GFE is tracked just as equipment purchased through the ECS Program. Upon receipt, equipment will be examined for transit damage, completeness, proper type, identification, and quantity. Operation and configuration logs are kept in accordance with the same procedures for equipment purchased through the ECS program. The government-assigned Equipment Control Number (ECN) will be maintained and used for identification and tracking purposes.

## **9.22 Government Acceptance**

Prior to submittal of each release of the ECS for NASA acceptance, the Quality Office ensures that deliverable contract hardware end-items, software, and final system documentation, including the Acceptance Data Package (DID 535/PA1), are in accordance with contract requirements. The Quality Office also verifies the closure of all nonconformances from the acceptance test program and participates in the Acceptance Review.

The Acceptance Data Package includes the following information with appropriate approvals:

- Records of the final system configuration audit, including the As-Built Configuration List of hardware and software (deviations from the as-designed configuration noted)
- Results of the system acceptance test program
- Test log books
- List of open items with reasons for items being open and appropriate authorization/approvals
- Deliverable data, instruction material, and equipment for maintenance and system test
- Operating manuals

This page intentionally left blank.

# Abbreviations and Acronyms

---

A <sub>o</sub>	Operational Availability
ADP	Automated Data Processing
ADPE	Automated Data Processing Equipment
AIT	Algorithm Integration & Test
ARC	Applied Research Corporation
ATRR	Acceptance Test Readiness Review
ATT	Acceptance Test Team
BOO	Business Operations Office
CCB	Configuration Control Board
CCR	Configuration Change Request
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CFR	Code Federal Regulations
CI	Configuration Item
CIL	Critical Items List
CIN	Configuration Identification Number
CM	Configuration Management
CMO	Configuration Management Organization
cmi	Continuous measurable improvement
CMS	Command Management Subsystem
COTS	Commercial-Off-The-Shelf
CRR	Capabilities Requirements Reviews
CSA	Configuration Status Accounting
CSMS	Communications and Systems Management Segment
CSR	Consent to Ship
CWBS	Contract Work Breakdown Structure
DAAC	Distributed Active Archive Center
DADS	Distributed Active Archive Center
DCMAO	Defense Contract Management Area Office
DCN	Document Change Notice

DID	Data Item Description
DM	Data Management
DMO	Data Management Organization
ECN	Equipment Control Number
ECP	Engineering Change Proposal
ECS	EOSDIS Core System
EDF	ECS Development Faculty
EDS	Electronic Data Systems
EGS	EOS Ground System
EMA	Enterprise Management Architecture
EOS	Earth Observing System
EOSDIS	Earth Observing System Data and Information System
ESD	Electrostatic Discharge
ESSi	Engineering and Science Services, Inc.
ETRR	Element Test Readiness Review
FMEA	Failure Modes and Effects Analysis
FOR	Flight Operations Review
FOS	Flight Operations Segment
FOT	Flight Operations Team
FRB	Failure Review Board
FRR	Flight Readiness Review
GATT	Government Acceptance Test Team
GFE	Government Furnished Equipment
GSA	Government Site Acceptance
GSFC	Goddard Space Flight Center
GSI	Government Source Inspection
GSORR	Ground System Operational Readiness Review
HAIS	Hughes Applied Information Systems, Inc.
HW	Hardware
I&T	System Integration and Test
IATO	Independent Acceptance Test Organization
ICC	Instrument Control Center
IDR	Incremental Design Review

ILS	Integrated Logistics Support
IV&V	Independent Verification and Validation
LCC	Lifecycle Cost
LRU	Line Replaceable Unit
LSA	Logistics Support Analysis
M&O	Maintenance and Operations
MDT	Mean Down Time
MOM	Mission Operations Manager
MOR	Mission Operations Manager
MR	Malfunction Report
MRB	Material Review Board
MTBF	Mean Time Between Failures
MTBM	Mean Time Between Maintenance
MTTR	Mean Time To Repair
NASA	National Aeronautics and Space Administration
NHB	NASA Handbook
NRCA	Nonconformance Reporting and Corrective Action
NYMA	NYMA Incorporated
PA	Performance Assurance
PAIP	Performance Assurance Implementation Plan
PAR	Performance Assurance Requirements
PDR	Preliminary Design Review
PGE	Product Generation Executable
PGS	Product Generation System
PHS&T	Packaging, Handling, Storage & Transportation
PI	Project Instruction
PMR	Project Management Review
PMS	Performance Measurement System
PTE	Portable Test Equipment
QA	Quality Assurance
QO	Quality Office
RDR	Release Design Review
RFP	Request for Proposal

RID	Review Item Discrepancy
RIR	Release Initiation Review
RMA	Reliability, Maintainability, and Availability
RRR	Release Readiness Review
SAM	System Assurance Manager
SCF	Science Computing Facility
SCG	Space Communication Group
SDPS	Science Data Processing Segment
SDR	System Design Review
SHEA	Safety, Health, and Environmental Affairs
SMC	System Management Center
SMO	Systems Management Office
SMO	Subcontract Management Office
SOAR	Spacecraft Orbital Anomaly Report
SORR	Segment Operational Readiness Review
SOW	Statement of Work
SRR	System Requirements Review
SSHA	System Safety Hazard Analysis
SSIP	System Safety Implementation Plan
SW	Software
TMDB	Technical Management Database
TMDE	Test Measurement Diagnostic Equipment
TRR	Test Readiness Review
V&V	Verification and Validation
VCATS	Vendor Costing and Tracking System
WBS	Work Breakdown Structure